



# **NAVAL POSTGRADUATE SCHOOL**

**MONTEREY, CALIFORNIA**

## **THESIS**

**SECURE REMOTE NETWORK ADMINISTRATION AND  
POWER MANAGEMENT**

by

Mark P. Sullivan

June 2004

Thesis Advisor:  
Second Reader:

Dale Courtney  
Dennis Volpano

**Approved for public release; distribution is unlimited**

THIS PAGE INTENTIONALLY LEFT BLANK

<b>REPORT DOCUMENTATION PAGE</b>			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.				
<b>1. AGENCY USE ONLY (Leave blank)</b>		<b>2. REPORT DATE</b> June 2004	<b>3. REPORT TYPE AND DATES COVERED</b> Master's Thesis	
<b>4. TITLE AND SUBTITLE:</b> Secure Remote Network Administration and Power Management			<b>5. FUNDING NUMBERS</b>	
<b>6. AUTHOR(S)</b> Mark P. Sullivan				
<b>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)</b> Naval Postgraduate School Monterey, CA 93943-5000			<b>8. PERFORMING ORGANIZATION REPORT NUMBER</b>	
<b>9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)</b> N/A			<b>10. SPONSORING/MONITORING AGENCY REPORT NUMBER</b>	
<b>11. SUPPLEMENTARY NOTES</b> The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
<b>12a. DISTRIBUTION / AVAILABILITY STATEMENT</b> Approved for public release; distribution is unlimited			<b>12b. DISTRIBUTION CODE</b>	
<b>13. ABSTRACT (maximum 200 words)</b> <p>Remote Network Administration allows network administrators to manage their networks while being physically separated from the network equipment. Having the capability to manage wired and wireless networks securely, from remote locations, can substantially reduce operating expenses across the entire Department of Defense</p> <p>A variety of methods for remotely managing networks is explored for both wired and wireless networks. Requirements for remote network administration are identified. Chief among them is security and the ability to remotely manage power. Several widely-used remote management utilities are examined. All fail to meet these two requirements. A new power control device is presented that can be managed securely and remotely.</p>				
<b>14. SUBJECT TERMS</b> Remote Network Administration, Network Management, Power Management			<b>15. NUMBER OF PAGES</b> 71	
			<b>16. PRICE CODE</b>	
<b>17. SECURITY CLASSIFICATION OF REPORT</b> Unclassified	<b>18. SECURITY CLASSIFICATION OF THIS PAGE</b> Unclassified	<b>19. SECURITY CLASSIFICATION OF ABSTRACT</b> Unclassified	<b>20. LIMITATION OF ABSTRACT</b> UL	

THIS PAGE INTENTIONALLY LEFT BLANK

**Approved for public release; distribution is unlimited**

**SECURE REMOTE NETWORK ADMINISTRATION AND POWER  
MANAGEMENT**

Mark P. Sullivan  
Captain, United States Air Force  
B.S., University of Maryland University College, 2000

Submitted in partial fulfillment of the  
requirements for the degree of

**MASTER OF SCIENCE IN COMPUTER SCIENCE**

from the

**NAVAL POSTGRADUATE SCHOOL  
June 2004**

Author: Mark P. Sullivan

Approved by: Dale Courtney  
Thesis Advisor

Dennis Volpano  
Second Reader

Peter Denning  
Chairman, Department of Computer Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

## **ABSTRACT**

Remote Network Administration allows network administrators to manage their networks while being physically separated from the network equipment. Having the capability to manage wired and wireless networks securely, from remote locations, can substantially reduce operating expenses across the entire Department of Defense

A variety of methods for remotely managing networks is explored for both wired and wireless networks. Requirements for remote network administration are identified. Chief among them is security and the ability to remotely manage power. Several widely-used remote management utilities are examined. All fail to meet these two requirements. A new power control device is presented that can be managed securely and remotely.

THIS PAGE INTENTIONALLY LEFT BLANK



## TABLE OF CONTENTS

<b>I.</b>	<b>INTRODUCTION.....</b>	<b>1</b>
<b>A.</b>	<b>OVERVIEW .....</b>	<b>1</b>
<b>B.</b>	<b>PROBLEM DEFINITION .....</b>	<b>1</b>
<b>C.</b>	<b>MOTIVATION .....</b>	<b>1</b>
<b>D.</b>	<b>OBJECTIVE .....</b>	<b>1</b>
<b>E.</b>	<b>SCOPE .....</b>	<b>2</b>
<b>F.</b>	<b>THESIS ORGANIZATION.....</b>	<b>2</b>
<b>II.</b>	<b>ELEMENTS OF WIRED AND WIRELESS NETWORKS.....</b>	<b>3</b>
<b>A.</b>	<b>INTRODUCTION.....</b>	<b>3</b>
<b>B.</b>	<b>WIRED NETWORK ELEMENTS .....</b>	<b>3</b>
1.	Topology.....	3
2.	Capabilities .....	4
3.	Star .....	4
4.	Bus .....	5
5.	Ring .....	6
6.	Mesh .....	6
<b>C.</b>	<b>WIRELESS NETWORK ELEMENTS .....</b>	<b>7</b>
1.	Capabilities .....	7
2.	Topology.....	8
3.	Equipment .....	10
<b>D.</b>	<b>CONCLUSION .....</b>	<b>10</b>
<b>III.</b>	<b>WIRELESS VS. WIRED NETWORK MANAGEMENT .....</b>	<b>13</b>
<b>A.</b>	<b>INTRODUCTION.....</b>	<b>13</b>
<b>B.</b>	<b>WIRED NETWORK MANAGEMENT UTILITIES/DEVICES.....</b>	<b>13</b>
1.	Telnet.....	13
2.	Secure Shell (SSH) .....	14
3.	Simple Network Management Protocol (SNMP) .....	15
4.	Remote Desktop .....	15
a.	Windows .....	16
b.	Virtual Network Computing (VNC) .....	16
c.	Citrix .....	17
d.	Virtual Private Network (VPN) .....	18
e.	Point-to-Point Tunneling Protocol (PPTP) .....	18
f.	Layer 2 Tunneling Protocol (L2TP).....	18
g.	Internet Protocol Security (IPSEC) .....	18
<b>C.</b>	<b>WIRELESS NETWORK MANAGEMENT UTILITIES/DEVICES.....</b>	<b>19</b>
<b>D.</b>	<b>CONCLUSION .....</b>	<b>21</b>
<b>IV.</b>	<b>REMOTE NETWORK MANAGEMENT AND ITS SECURITY RISKS .....</b>	<b>23</b>
<b>A.</b>	<b>INTRODUCTION.....</b>	<b>23</b>
<b>B.</b>	<b>WIRED NETWORK REMOTE MANAGEMENT UTILITIES.....</b>	<b>24</b>
1.	Telnet.....	24

2.	SSH .....	25
3.	SNMP .....	26
4.	Remote Desktop Utilities .....	26
a.	Windows Remote Desktop Protocol.....	26
b.	Virtual Network Computing (VNC) .....	27
c.	Citrix .....	30
d.	GoToMyPC.....	31
5.	VPN .....	33
a.	Point-to-Point Tunneling Protocol (PPTP) .....	33
b.	Layer 2 Tunneling Protocol.....	33
c.	Internet Protocol Security.....	33
d.	L2TP + IPSec .....	34
e.	Tunneling .....	34
C.	WIRELESS NETWORK REMOTE MANAGEMENT UTILITIES.....	35
D.	CONCLUSION .....	39
V.	DEVICES LACKING NETWORK MANAGEMENT (OR THE WEAK LINK) .....	41
A.	INTRODUCTION.....	41
B.	TAKING CONTROL OF YOUR POWER.....	41
C.	BACKUP METHODS OF REMOTE POWER REBOOTING .....	43
D.	CONCLUSION .....	49
VI.	CONCLUSION .....	51
A.	RESEARCH CONCLUSION .....	51
B.	RECOMMENDATIONS FOR FURTHER RESEARCH .....	52
	LIST OF REFERENCES.....	53
	INITIAL DISTRIBUTION LIST .....	55

## LIST OF FIGURES

Figure 2.1.	Star Topology (From: <a href="http://www.delmar.edu/Courses/ITNW2313/network.htm">http://www.delmar.edu/Courses/ITNW2313/network.htm</a> , May 2004).....	4
Figure 2.2.	Bus Topology (From: <a href="http://www.delmar.edu/Courses/ITNW2313/network.htm">http://www.delmar.edu/Courses/ITNW2313/network.htm</a> , May 2004).....	5
Figure 2.3.	Ring Topology (From: <a href="http://www.delmar.edu/Courses/ITNW2313/network.htm">http://www.delmar.edu/Courses/ITNW2313/network.htm</a> , May 2004).....	6
Figure 2.4.	Mesh Topology (From: <a href="http://www.delmar.edu/Courses/ITNW2313/network.htm">http://www.delmar.edu/Courses/ITNW2313/network.htm</a> , May 2004).....	7
Figure 2.5.	<i>Ad hoc</i> (peer to peer) vs. Infrastructure (base station) (From: Gast. <i>802.11 Wireless Networks – The Definitive Guide</i> . (O’Reilly, 2002), 11) .....	8
Figure 2.6.	<i>Ad hoc</i> Wireless Network (From: <a href="http://www.informit.com/articles/article.asp?p=101591">http://www.informit.com/articles/article.asp?p=101591</a> , May 2004) .....	9
Figure 2.7.	Typical Hybrid Network Diagram Showing Wireless and Wired Access (From: Gast. <i>802.11 Wireless Networks – The Definitive Guide</i> . O’Reilly, 2002, 11) .....	10
Figure 3.1.	Telnet Login from Command Prompt .....	13
Figure 3.2.	PuTTY SSH Client .....	14
Figure 3.3.	SSH Login on Router-Based SSH Server .....	15
Figure 3.4.	Router System Log Showing Login Process .....	15
Figure 3.5.	VNC Login Prompts .....	16
Figure 3.6.	Remote VNC Desktop on Top of Local Desktop .....	17
Figure 3.7.	Web-Based Management Tool for Linksys WAP (From: <a href="http://www.linksys.com">www.linksys.com</a> , May 2004).....	20
Figure 3.8.	SNMP Client Software .....	21
Figure 4.1.	Test-Bed Network developed for thesis testing.....	23
Figure 4.2.	Telnet Login Password (Cisco) Shown in cleartext (From: <a href="http://www.ethereal.com">www.ethereal.com</a> , May 2004).....	24
Figure 4.3.	Initial SSH Connection Shows Server Fingerprint .....	25
Figure 4.4.	VNC Server Configuration .....	27
Figure 4.5.	PuTTY Connections.....	28
Figure 4.6.	PuTTY SSH Version and Compression.....	28
Figure 4.7.	PuTTY Tunnel Configuration.....	29
Figure 4.8.	PuTTY Session Configuration.....	30
Figure 4.9.	VNC Remote Login through SSH Tunnel.....	30
Figure 4.10.	Citrix ICA 128-bit Encryption Configuration.....	31
Figure 4.11.	GoToMyPC circumvents firewall policies .....	32
Figure 4.12.	Wireless Access Points in DMZ (From: Osbourne. <i>CWNA, Certified Wireless Network Administrator</i> . McGraw Hill, 2003, 418) .....	36
Figure 4.13.	Common Wired Backbone (From: Osbourne. <i>CWNA, Certified Wireless Network Administrator</i> . McGraw Hill, 2003, 101) .....	36

Figure 4.14.	Wireless Bridge (From: Osbourne. CWNA, Certified Wireless Network Administrator. McGraw Hill, 2003, 102) .....	37
Figure 5.1.	Web-Based Interface Rebooter (From: <a href="http://www.wti.com">http://www.wti.com</a> , May 2004) .....	42
Figure 5.2.	Remotely Manageable UPS is Unreachable Due to Key Router Being Down.....	43
Figure 5.3.	Command Line Interface for Remote Rebooter (From: <a href="http://www.wti.com">http://www.wti.com</a> , May 2004).....	44
Figure 5.4.	UPS with Built-In Modem for Remote Management .....	45
Figure 5.5.	UPS with Remote Management via Built-in Touchtone Controller .....	46
Figure 5.6.	Backup Power Supply Controlled by Server Loaded with Heartbeat Software .....	47
Figure 5.7.	Backup Power Supply with Built-in Auto-Rebooter .....	48
Figure 5.8.	Backup Power Supply with Built-In Auto-Rebooter and Backup Management.....	49

## LIST OF ABBREVIATIONS, ACRONYMS AND SYMBOLS

<b>APC</b>	American Power Conversion
<b>ATM</b>	Asynchronous Transfer Mode
<b>AH</b>	Authentication Header
<b>ESP</b>	Encapsulating Security Payload
<b>EAP-TLS</b>	Extensible Authentication Protocol - Transport Layer Security
<b>ICMP</b>	Internet Control Message Protocol
<b>IETF</b>	Internet Engineering Task Force
<b>IKE</b>	Internet Key Exchange
<b>IP</b>	Internet Protocol
<b>IPSEC</b>	Internet Protocol Security
<b>L2F</b>	Cisco's Layer 2 Forwarding
<b>L2TP</b>	Layer 2 Tunneling Protocol
<b>LAN</b>	Local Area Network
<b>NAT</b>	Network Address Translation
<b>PPP</b>	Point-to-Point Protocol
<b>PPTP</b>	Point-to-Point Tunneling Protocol
<b>RDP</b>	Remote Desktop Protocol
<b>SSH</b>	Secure Shell
<b>SSL</b>	Secure Socket Layer
<b>SNMP</b>	Simple Network Management Protocol
<b>TCP</b>	Transmission Control Protocol
<b>UPS</b>	Uninterruptible Power Supply
<b>UDP</b>	User Datagram Protocol
<b>VLAN</b>	Virtual Local Area Network
<b>VNC</b>	Virtual Network Computing
<b>VPN</b>	Virtual Private Network
<b>WEP</b>	Wired Equivalent Privacy
<b>WAP</b>	Wireless Access Point

THIS PAGE INTENTIONALLY LEFT BLANK

## **ACKNOWLEDGMENTS**

I would like to thank my advisors, the NPS Staff, AFIT Staff, and my fellow students for the opportunity to learn.

THIS PAGE INTENTIONALLY LEFT BLANK



# **I. INTRODUCTION**

## **A. OVERVIEW**

This thesis explores the many methods of remote network administration for both wired and wireless networks. This project is undertaken in an effort to provide the Department of Defense several solutions for secure remote network administration. Specifically, this thesis researches the necessary components that enable complete and secure network administration from a remote location.

## **B. PROBLEM DEFINITION**

Performing network administration remotely, from a central location, is possible. However, for each service opened in a firewall, there is another potential vulnerability, which may be exploitable by hackers. To perform remote network administration *securely* is the true problem researched in this thesis.

## **C. MOTIVATION**

The Department of Defense is continually pushed to do more with less. In this effort, more and more locations are becoming administered from central locations, normally within the same geographic area. To reduce the required manpower further, it is necessary to push the management even further away, sometimes leaving an area completely unmanned.

In order to enable centralized management, from geographically separated locations, remote management tools must be implemented. These tools must be all encompassing, flexible, and most importantly, *secure*.

## **D. OBJECTIVE**

In support of the Department of Defense's objectives, this thesis surveys several methods for secure remote network administration. Remote network administration greatly reduces the manning required for the day-to-day maintenance of our networks. This thesis also investigates any possible weak-links with remote administration and attempts to identify automated processes to deal with them. Lastly, this thesis will attempt to build a test bed to incorporate the recommended utilities and/or hardware.

## **E. SCOPE**

This thesis will research, and test when possible, open-source, freeware, and widely available remote network management utilities. The focus being on cost savings, this thesis will test commercial off the shelf software that is already incorporated into widely used operating systems throughout the Department of Defense, such as Windows XP Professional and Windows Server 2003.

## **F. THESIS ORGANIZATION**

This thesis is organized into six chapters. Chapter II discusses background information pertaining to wired and wireless networks. Specifically, it discusses the topology, equipment, and capabilities of each. Chapter III discusses wired and wireless network management tools. Chapter IV discusses how to effectively, and securely, use the tools outlined in Chapter III. Chapter V discusses those devices, which support networks, but are not normally network manageable. Specifically, it discusses remote power management and an automated method of reducing downtime. Chapter VI is the conclusion. It discusses the results of the test bed and recommends topics for future research.

## **II. ELEMENTS OF WIRED AND WIRELESS NETWORKS**

### **A. INTRODUCTION**

In order for computers to communicate with one another and share resources, they must somehow connect to each other, either in the form of a wired or wireless connection. Regardless of the connection, a typical network has several key components including networking cards, cabling, routers, and switches, as well as bridges, gateways, firewalls, servers, and backup power supplies. These devices not only comprise a network, but also establish communication between all devices including client workstations and shared resources such as printers and scanners.

### **B. WIRED NETWORK ELEMENTS**

#### **1. Topology**

Network topology refers to the arrangement or physical layout of computers, cables, and other components on the network. Topology is a commonly used term by network professionals when referring to the network's basic design. Topologies can be physical (cabling) or logical (how they work). Topology is synonymous with words such as physical layout, design, diagram, and map.<sup>1</sup>

Topology is a key factor when determining network capabilities. Each different topology has its own capabilities and affects the equipment needed, future growth potential of a network, and most importantly, the management of the network.

Primary topologies include star, bus, ring, and mesh. A star topology forms when computers connect to wired segments, which branch out from a single point. A bus topology forms when each connected device shares a common wire (cable). A ring topology is computers connected to a wire that forms a loop. All devices connecting directly to all other devices form a mesh topology. Furthermore, two or more of the above standard topologies used together can comprise a hybrid method for networking as well.<sup>2</sup>

---

<sup>1</sup> Tamar Dean, *Enhanced Network+ Guide to Networks*. Enhanced Edition, (Course Technology, 2003), 178.

<sup>2</sup> Forouzan, *Data Communications and Networking*. 2<sup>nd</sup> Edition, (McGraw Hill, 2001), 22.

## 2. Capabilities

The selection of hardware and cabling will affect the overall network performance for each of the network topologies. For example, fiber has a higher throughput than coaxial cable. Other factors affecting network performance are the types of operating systems, client/server applications, and distances between devices.

## 3. Star

Since all network communications must flow through a central connection device, centralized management is an obvious advantage to the star topology. It is also a possible weakness since a single-point-of-failure now exists. Depending on the physical locations of all network devices, the star topology may demand a higher amount of cabling to allow all devices to connect back to the central device. However, since all devices possess individual connections back to the central device, a single computer failure will not affect the rest of the network.<sup>3</sup>

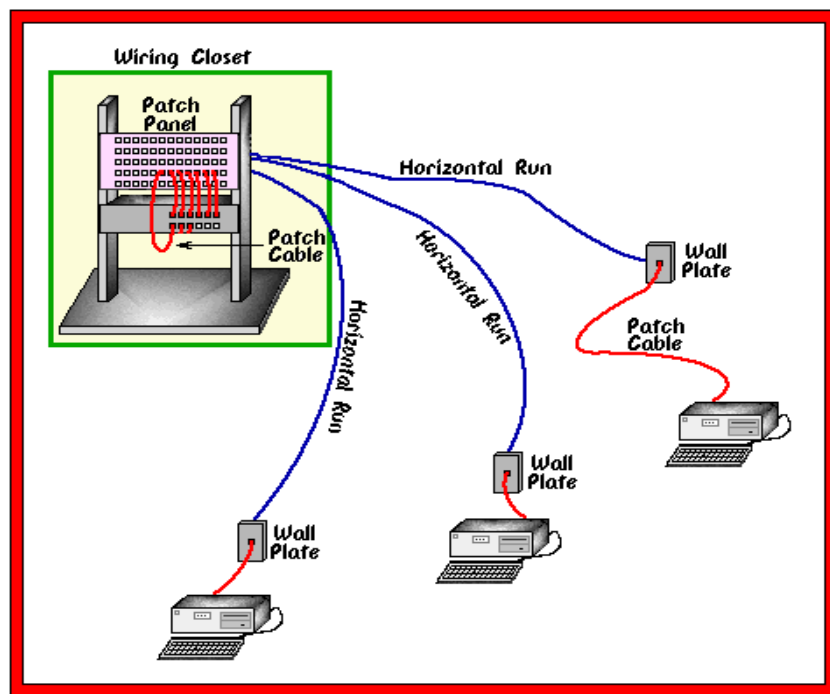


Figure 2.1. Star Topology (From: <http://www.delmar.edu/Courses/ITNW2313/network.htm>, May 2004)

<sup>3</sup> Feibel, *Encyclopedia of Networking*. Network Press. (Sybex, 2000), 1166

#### 4. Bus

Only one computer can transmit at a time on a bus network. Therefore, the number of computers attached to a single bus will affect the overall network performance. In a bus network, each computer is not responsible for passing data from one computer to the next. As with star topology, the failure of one computer will not affect the other devices connected to the same bus. Data passes from one device to the next by transmitting the data onto the bus with an address for the specific recipient. The use of a “terminator” stops the signal bounce, or otherwise, this data will continue to bounce from one end of the bus to the other. A terminator may be a hardware device, or even another computer, which is designed to absorb the signal thereby preventing bounce back. In any case, the bus must not have unterminated ends, which would cause bounce back of the signal, disallowing any further data to enter the bus. If a break in the bus occurs at any point, an unterminated endpoint will result, and therefore, all network communication will stop due to bounce back. Each computer will still function but will not have network communication capability.<sup>4</sup>

Network growth is possible by either installing a completely new bus line or by extending the current bus. The use of a connector can cause an extension (i.e. barrel connector). Connectors introduce resistance and therefore weaken the signal. Using excessive connectors without the use of a repeater can affect network performance detrimentally. A repeater is essentially an amplifier used in series to boost the signal.

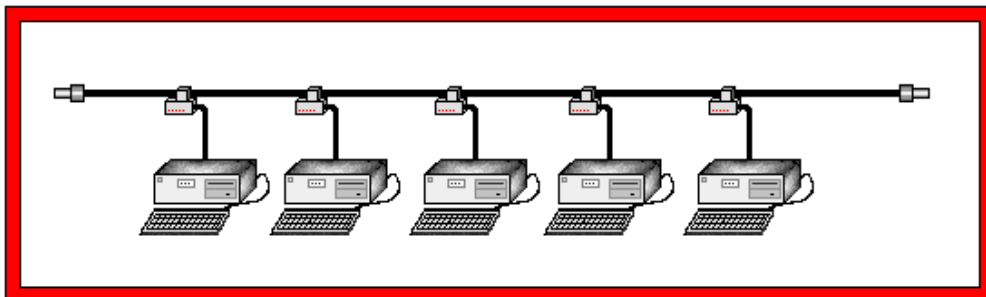


Figure 2.2. Bus Topology (From: <http://www.delmar.edu/Courses/ITNW2313/network.htm>, May 2004)

---

<sup>4</sup> Tanenbaum. *Computer Networks*. (Prentice Hall, 2003), 17

## 5. Ring

A ring topology is often confused with a bus topology when the bus connects at both ends. However, a ring topology is different from a bus topology. The data passes along the ring in one direction and passes through each computer in a ring topology. Each computer receives the signal, determines if the data is destined for itself or not, and if not, will retransmit the signal out to the next computer in the ring. Therefore, the failure of a single computer will impact the entire network.<sup>5</sup>

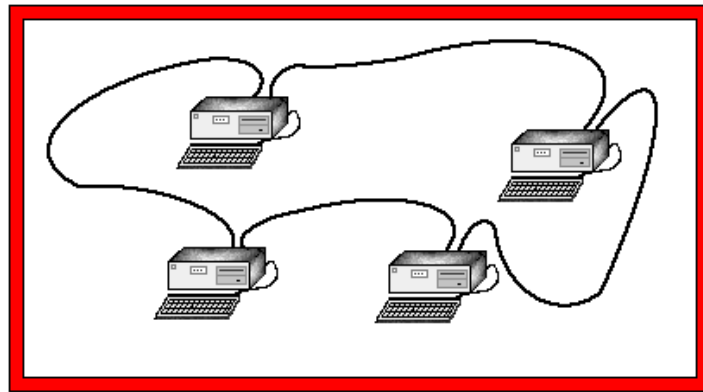


Figure 2.3. Ring Topology (From: <http://www.delmar.edu/Courses/ITNW2313/network.htm>, May 2004)

## 6. Mesh

A mesh topology is superior to the bus, ring, and star. Since each computer connects to every other computer in the network directly, a greater level of redundancy and reliability exists. If one connection fails between computer A and computer B, many redundant paths are still available for communication to continue between computer A and computer B. Cost is the main disadvantage to a mesh topology. Connecting every device to one another requires a great deal of cabling. The cost of this cabling makes the mesh network prohibitive to a majority of network planners.<sup>6</sup>

---

<sup>5</sup> Feibel, *Encyclopedia of Networking*. Network Press, (Sybex, 2000), 1165.

<sup>6</sup> Tamar Dean. *Enhanced Network+ Guide to Networks*, Enhanced Edition. (Course Technology, 2003), 191.

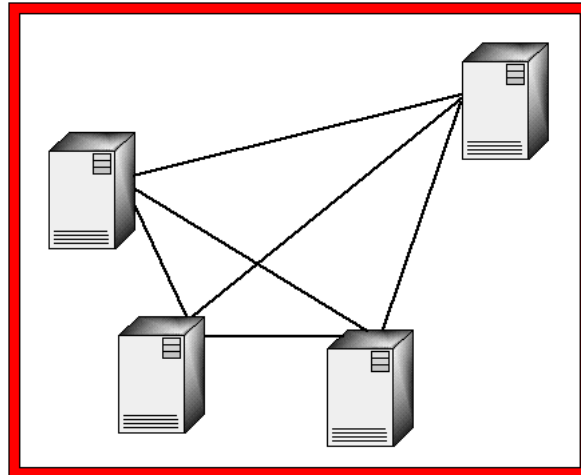


Figure 2.4. Mesh Topology (From: <http://www.delmar.edu/Courses/ITNW2313/network.htm>, May 2004)

### C. WIRELESS NETWORK ELEMENTS

The initial planning for the deployment of a wireless network is more difficult than planning a wired network deployment. A wired network only requires cables be run to the associated network device for backbone connectivity. The deployment of wireless networks requires many more factors to consider over traditional wired networks.

Besides the RF issues inherent to wireless networks, it is also necessary to consider the interfaced wired network. In most cases, the wireless network will extend the reach of a wired network. Therefore, the stability of the wired network is crucial to wireless network stability as well.<sup>7</sup> Although the initial planning may be more difficult and time consuming, it does result in decreased overall time and costs to provide network connectivity to expanded customers and devices.

#### 1. Capabilities

Wireless networks allow clients and network devices to connect to the network without a hardwire cable, either for ease or necessity. When initially deploying a network with a non-existent hardwire backbone, it is possible to establish a wireless network in a short time allowing immediate network connectivity for users and associated network devices. It would be a perfect application for a military field deployment if a hardwire Ethernet backbone does not already exist. Wireless networking would also allow for a mobile deployment, as it will not be necessary to roll out or roll in cabling.

---

<sup>7</sup> Gast. *802.11 Wireless Networks – The Definitive Guide*. (O'Reilly, 2002), 293.

Wireless networks have two different modes: infrastructure and *ad hoc*. The *ad hoc* network provides connectivity directly between network devices without the need for a common access point. The infrastructure mode is the most common wireless network in use, which uses an access point for relaying information to and from wireless clients.

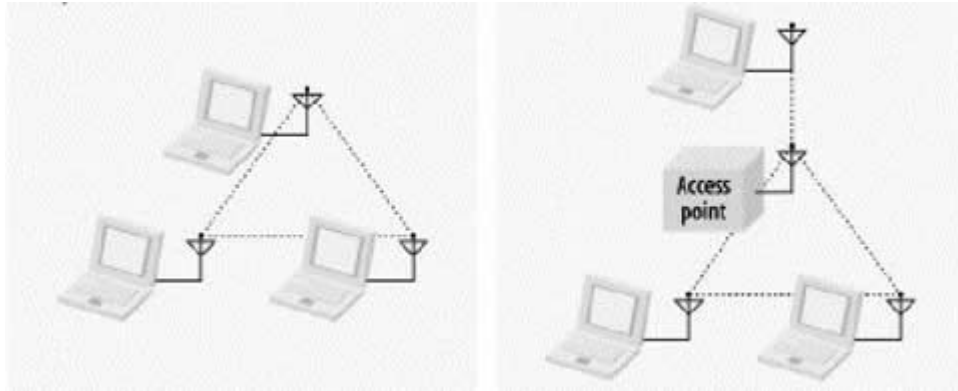


Figure 2.5. *Ad hoc* (peer to peer) vs. Infrastructure (base station) (From: Gast. 802.11 *Wireless Networks – The Definitive Guide*. (O'Reilly, 2002), 11)

Wireless networks allow for expansion to a pre-existing wired network. This reduces cost by eliminating expensive cabling and greatly reducing the time needed for providing network connectivity to expanded users and devices.

Allowing roaming between access points depends on the wireless network's purpose. This would be especially beneficial within buildings, but not necessarily between buildings as this may pose a security risk. Roaming would allow a client device (i.e. laptop) to stay connected while moving from, for example, an office to the conference room, without having to reestablish the network connection.

## 2. Topology

Wireless network topologies refer to the manner in which the wireless devices communicate with each other and other network devices. *Ad hoc* networks are normally established for a specific purpose (i.e. collaborating) and for a short period.<sup>8</sup> (See Figure 2.6.)

---

<sup>8</sup> Gast. 802.11 *Wireless Networks – The Definitive Guide*. (O'Reilly, 2002), 11.



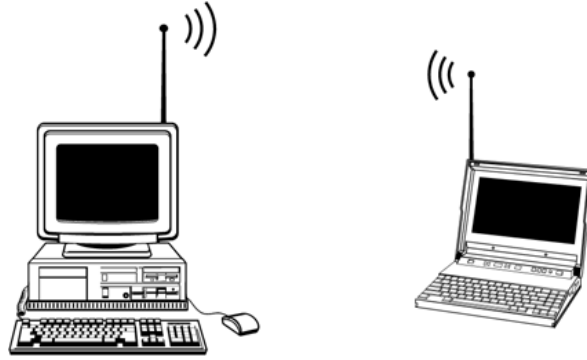


Figure 2.6. *Ad hoc Wireless Network* (From: <http://www.informit.com/articles/article.asp?p=101591>, May 2004)

Figure 2.7 shows a typical wireless network interfacing with a corporate LAN. It is important to note that the physical connection of each Access Point is not necessarily on a separate wired backbone. The wired backbone may be the same backbone servicing the entire internal network, but possibly separated virtually for security purposes by statically assigning the Access Points IPs in a subnet separate from the wired internal LAN. Separating the access points from internal LAN devices allows the implementation of more stringent security rules for wireless access clients.

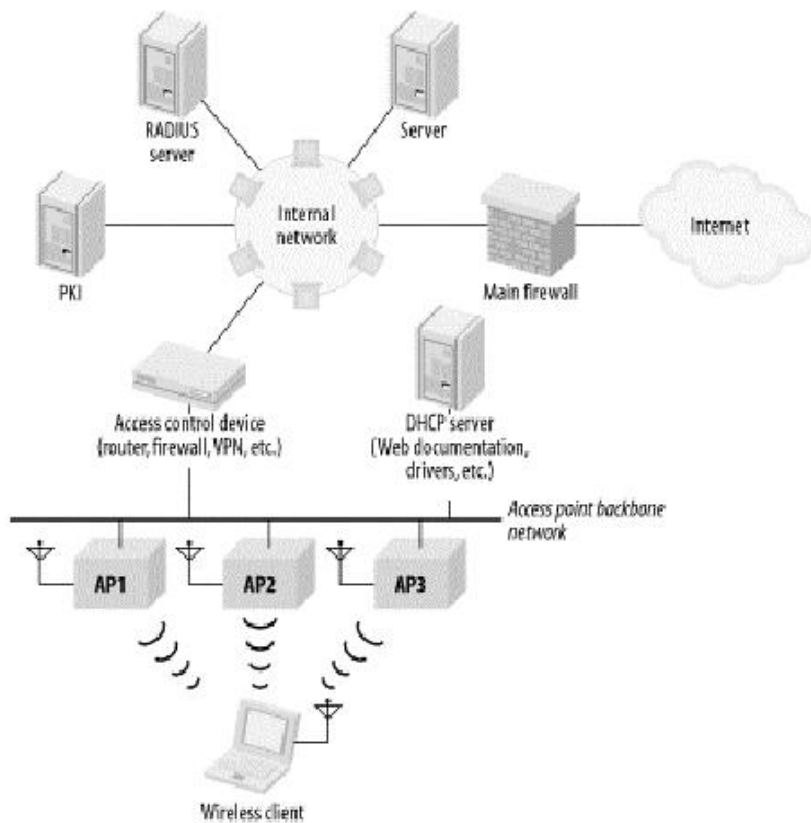


Figure 2.7. Typical Hybrid Network Diagram Showing Wireless and Wired Access  
(From: Gast. 802.11 Wireless Networks – The Definitive Guide. O’Reilly, 2002, 11)

### 3. Equipment

*Ad hoc* wireless networks require a wireless NIC at each client device, in the form of a PCMCIA card, internal wireless NIC, or external wireless NIC. Infrastructure wireless networks need at least one access point in addition to wireless NICs at each client device. In most cases, a wireless network will interface with a pre-existing wired LAN. Building a network from scratch also requires all the aforementioned equipment for wired networks.

### D. CONCLUSION

Functional requirements, the size of the network, standards, and funds available are some of the factors to consider when deciding on a network topology. Network topology should always be determined early in the design phase. Pros and cons exist for each topology. However, the ease of adding and removing computers, the centralized

monitoring and management, and the reduction of network outages due to single device failure are the reasons that the star topology is the most used.

Wireless technology is improving rapidly and along with that is its popularity. Many different wireless solutions would be beneficial to the Department of Defense, ranging from roaming within a warehouse, building-to-building connectivity, and highly mobile field deployments.<sup>9</sup>

When deciding between wired and wireless networks, you must take into consideration start-up costs, functionality, security, and remote management capability. The next chapter discusses the different management interfaces possible with wired and wireless networks.

---

<sup>9</sup> Osbourne. *CWNA, Certified Wireless Network Administrator*. Chapter 1, (McGraw Hill, 2003).

THIS PAGE INTENTIONALLY LEFT BLANK

### III. WIRELESS VS. WIRED NETWORK MANAGEMENT

#### A. INTRODUCTION

The first step in network management is to decide on the kind of network—wired, wireless, or both—and the network topology. The next step is the type of equipment used to implement the network design. It is important to choose the network devices carefully in order to have a central management system also capable of remote management. For cost and simplicity, it would be best to choose the network devices based on some common management functionality, for example, SSH capability. This chapter discusses the most common network management utilities.

#### B. WIRED NETWORK MANAGEMENT UTILITIES/DEVICES

##### 1. Telnet

Telnet is by far the most popular way to configure a network device remotely since telnet is now included in almost every network device available. It is possible to initiate a telnet session from almost any command prompt (see Figure 3.1). The remote administrator can gain access to a command line interface by simply entering a username and password. From the command line interface, the remote administrator can perform actions from router configuration to reboot procedures. Most network devices are accessible and manageable via the telnet interface.<sup>10</sup>

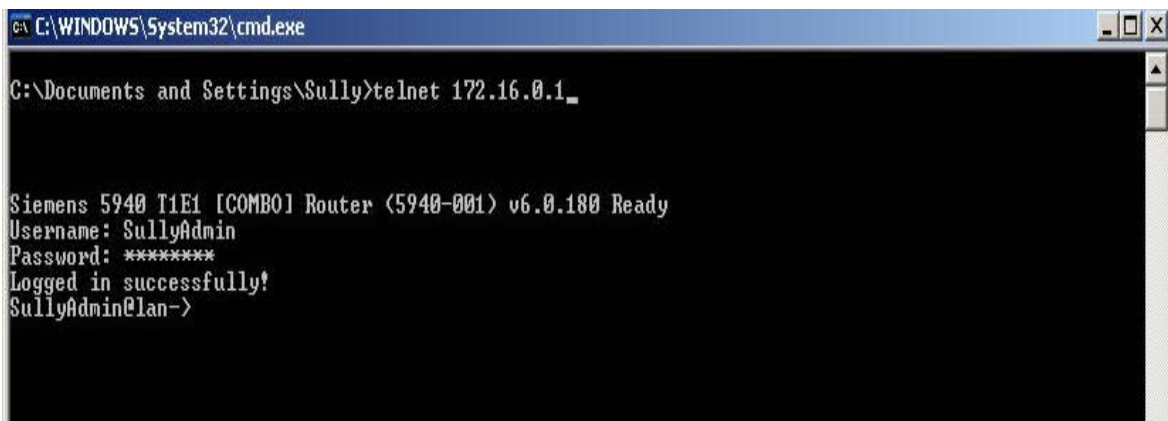


Figure 3.1. Telnet Login from Command Prompt

---

<sup>10</sup> Forouzan, *Data Communications and Networking*, 2<sup>nd</sup> Edition, (McGraw Hill, 2001), 742.

## 2. Secure Shell (SSH)

SSH is nothing more than secure telnet. SSH uses public key-based authentication or strong encryption to protect the username and password during the authentication process. Once authenticated, the remote administrator has the same capabilities as if using the telnet interface, while the entire process is encrypted. Telnet, rlogin, and other insecure remote utilities can use SSH as a replacement. To use SSH, the source must have a SSH client such as freeware PuTTY (see Figure 3.2) and the destination must have a SSH server. Most Unix/Linux systems have a SSH server built into the operating system. Windows does not have a built-in SSH server. Therefore, it is necessary to use a third party SSH server, such as the freeware OpenSSH (<http://sshtools.sourceforge.net/>), or commercial SSH Tectia (<http://www.ssh.com>).<sup>11</sup>

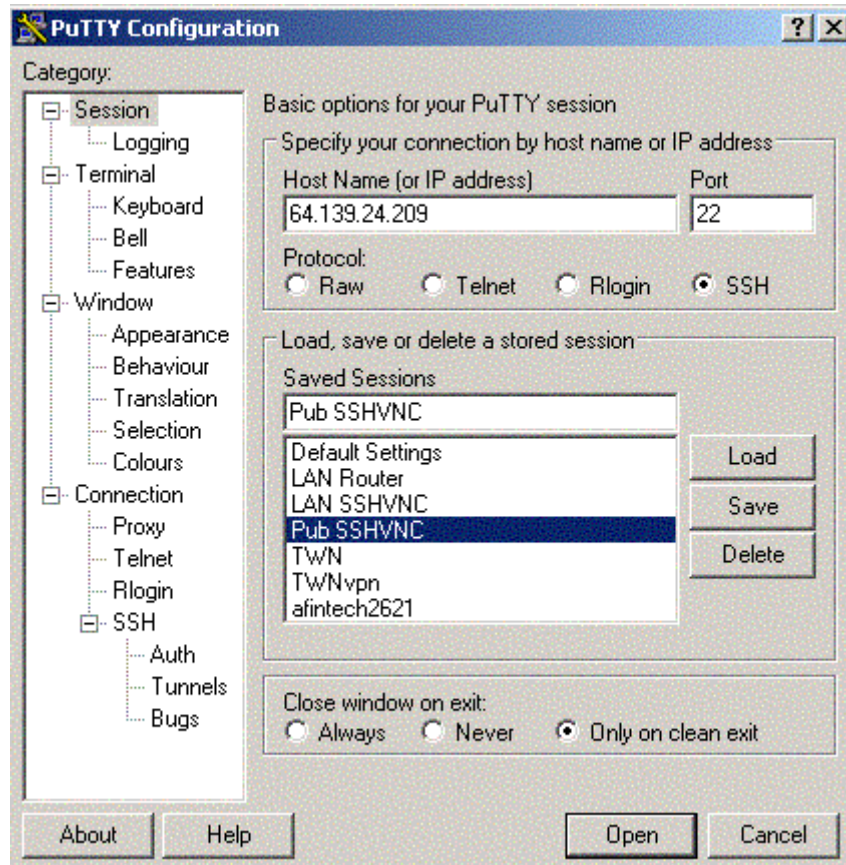
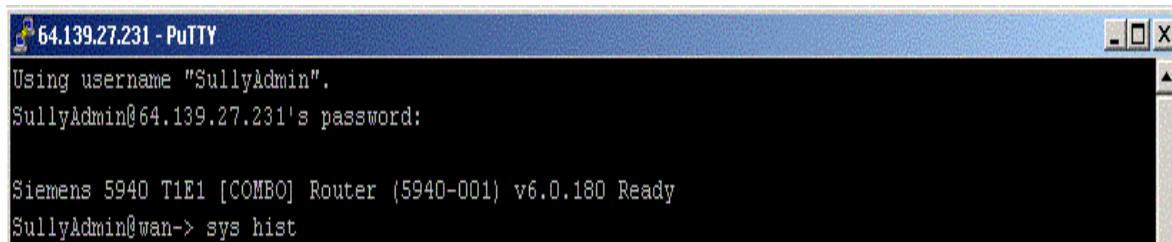


Figure 3.2. PuTTY SSH Client

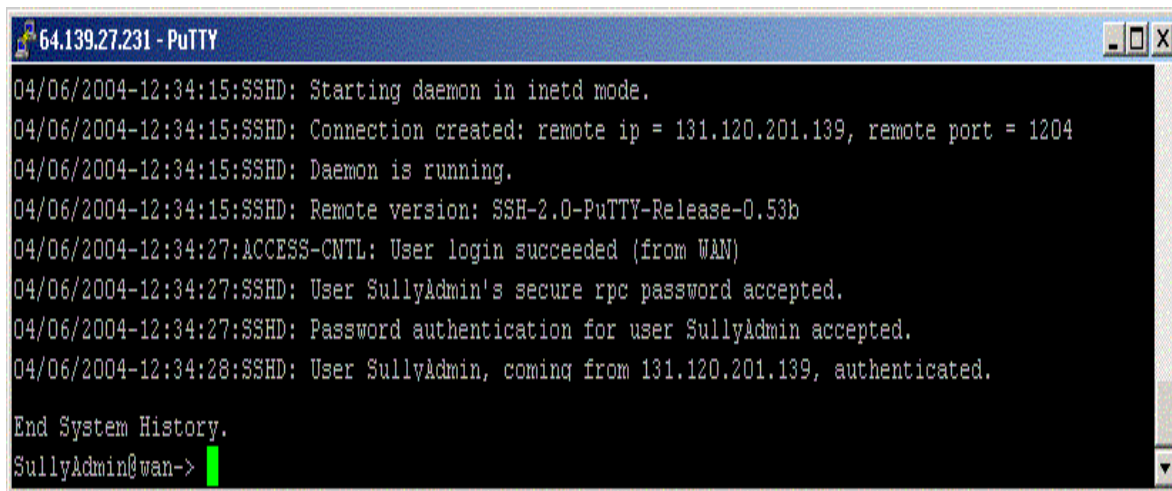
<sup>11</sup> Northcutt, Zeltser, Winters, Frederick, and Ritchey. *Inside Network Perimeter Security*. (New Riders, 2003), 145.



```
64.139.27.231 - PuTTY
Using username "SullyAdmin".
SullyAdmin@64.139.27.231's password:

Siemens 5940 T1E1 [COMBO] Router (5940-001) v6.0.180 Ready
SullyAdmin@wan-> sys hist
```

Figure 3.3. SSH Login on Router-Based SSH Server



```
64.139.27.231 - PuTTY
04/06/2004-12:34:15:SSHD: Starting daemon in inetd mode.
04/06/2004-12:34:15:SSHD: Connection created: remote ip = 131.120.201.139, remote port = 1204
04/06/2004-12:34:15:SSHD: Daemon is running.
04/06/2004-12:34:15:SSHD: Remote version: SSH-2.0-PuTTY-Release-0.53b
04/06/2004-12:34:27:ACCESS-CNTL: User login succeeded (from WAN)
04/06/2004-12:34:27:SSHD: User SullyAdmin's secure rpc password accepted.
04/06/2004-12:34:27:SSHD: Password authentication for user SullyAdmin accepted.
04/06/2004-12:34:28:SSHD: User SullyAdmin, coming from 131.120.201.139, authenticated.

End System History.
SullyAdmin@wan->
```

Figure 3.4. Router System Log Showing Login Process

### 3. Simple Network Management Protocol (SNMP)

SNMP is a tool (protocol) that allows remote and local management of items on the network including servers, workstations, routers, switches, and other managed devices. SNMP has been around since 1988 and has evolved through many versions, the most popular of which are SNMP version 1 and SNMP version 3. Many different management products use SNMP to manage geographically separated network devices.<sup>12</sup>

### 4. Remote Desktop

Remote Desktop utilities allow a user to connect to a remote computer and use this computer as if sitting in front of it. Remote Desktop utilities make it possible to see the GUI of the remote PC's operating system through streaming graphics back to the local PC, presenting the graphics within the remote desktop utility window. In turn, the mouse clicks/movements and keystrokes are sent to the remote PC. A username and password authenticate most remote desktop utilities (see Figure 3.5). Several different types of terminal services, (also known as remote desktop utilities) exist.

---

<sup>12</sup> Ibid., 148 and 474.

**a. Windows**

Windows Remote Desktop allows access to a Windows session running on a computer from a remote location. This provides a connection to a work computer from home and access to all applications, files, and network resources as if sitting in front of the work computer. The remote user is actually controlling a specific machine, not a virtual profile, such as it is with Citrix.

**b. Virtual Network Computing (VNC)**

VNC is freeware software that makes it possible to view and fully-interact with one computer from any other remote computer or mobile device. VNC software is cross-platform capable, which allows remote control between different types of computer and operating systems. Any desktop can be controlled remotely from within a browser via the Java viewer without having to install software (see Figure 3.6). VNC includes both the client-side and server-side software in one package. The network administrator can choose to enable the server side on any machines configured for remote control. VNC has a wide range of applications including system administration, IT support, and helpdesks. The system allows several connections to the same desktop, providing an invaluable tool for collaborative or shared working in the workplace or classroom.<sup>13</sup>



Figure 3.5. VNC Login Prompts

<sup>13</sup> <http://www.realvnc.com> (May 2004)



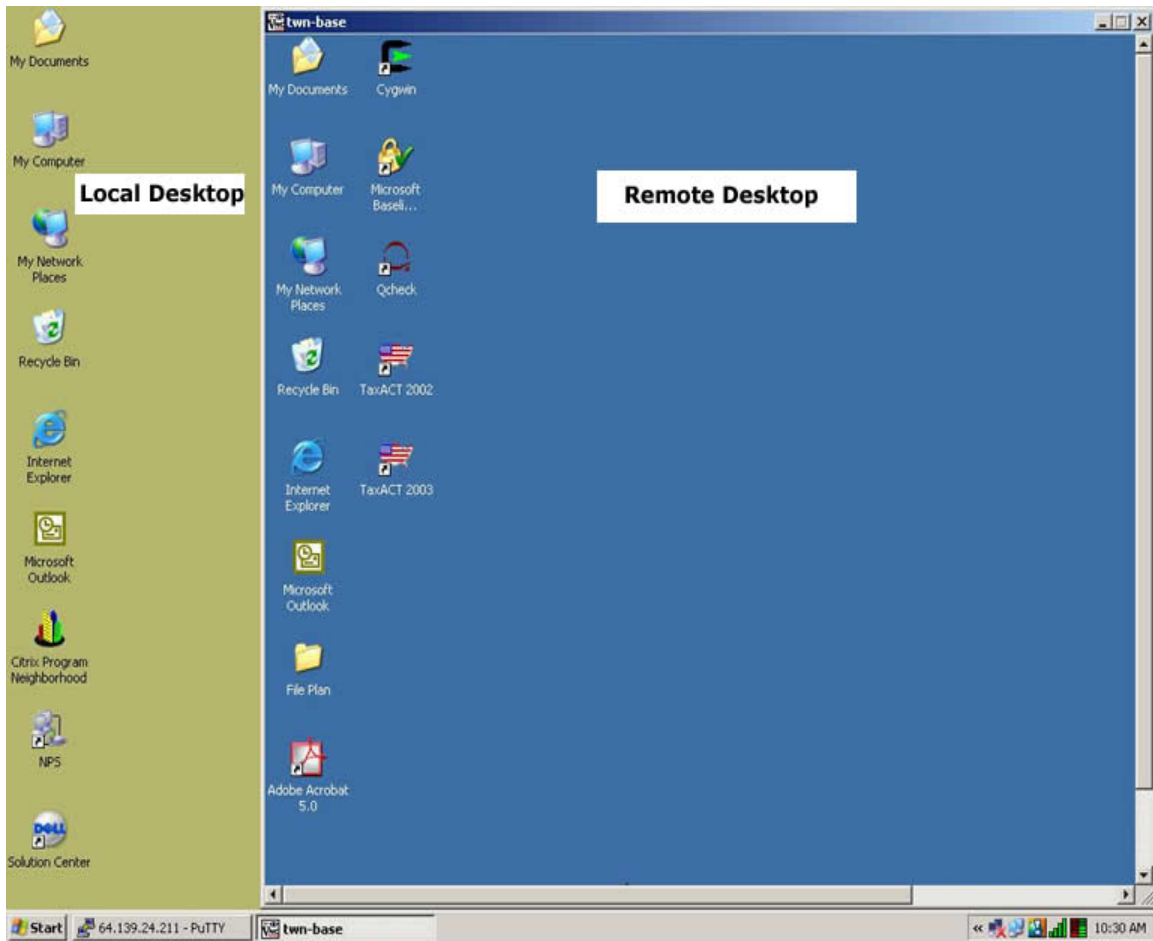


Figure 3.6. Remote VNC Desktop on Top of Local Desktop

*c. Citrix*

The Citrix MetaFrame Access Suite is a commercial program allowing Windows programs to run on another machine as if it were running on a personal machine. The computer's keyboard, mouse, and monitor are used for interacting with the program, but the actual processing happens on a remote computer. The user installs a Citrix client that interacts with the Citrix server. The configuration of a separate server with the Citrix Server software illustrates the difference between Citrix MetaFrame Access Suite and VNC or Windows Remote Desktop. When clients log into the Citrix server, clients will see their network profile desktop, not a specific computer's desktop.<sup>14</sup>

<sup>14</sup> <http://www.citrix.com> (May 2004).

Citrix has recently bought out goToMyPC.com, and the combination of Citrix and GoToMyPC's web-based remote access is now even better. Instead of installing client software on the local PC, it is now possible to access the remote access servers via GoToMyPC's website. GoToMyPC Corporate also has complete online administration for managing an employee's remote-access privileges.

**a. *Virtual Private Network (VPN)***

VPN provides users a secure link to access a corporate network over the Internet or other public or private networks without the expense of leased lines. A VPN is secured by a combination of tunneling, encryption, authentication, access control, and auditing technologies/services used to transport traffic over the Internet or any insecure network that uses the TCP/IP protocol suite for communication. The three most popular VPN technologies are PPTP, IPsec, and L2TP.<sup>15</sup>

**b. *Point-to-Point Tunneling Protocol (PPTP)***

PPTP is a PPP tunneling protocol designed to allow PPP links to terminate over a routed network upstream from a NAS. The protocol was defined by the PPTP forum (a group of computer technology manufacturers including Microsoft, US Robotics, Ascend, and 3Com). PPTP encapsulates PPP packets within Internet Protocol (IP) packets using GRE making forwarding over any IP network possible. Unlike IPsec, PPTP does not specify any security for tunneled traffic. One great advantage of PPTP over IPsec is that PPTP works through NAT. Another advantage is its integration with many hardware devices and is widely available in operating systems.

**c. *Layer 2 Tunneling Protocol (L2TP)***

L2TP is also PPP tunneling protocol. RFC 2661 defines L2TP and takes the best of Cisco's Layer 2 Forwarding (L2F) protocol and PPTP. L2TP can send encapsulated PPP packets over IP, x.25, frame relay, or ATM networks.

**d. *Internet Protocol Security (IPSEC)***

IPsec runs at the network layer and provides authentication and encryption as defined by the Internet Engineering Task Force (IETF). By using a combination of Internet Key Exchange (IKE), Encapsulating Security Payload (ESP), and Authentication Header (AH), IPsec can protect any protocol that runs on top of IP, such

---

<sup>15</sup> Northcutt, Zeltser, Winters, Frederick, and Ritchey. *Inside Network Perimeter Security*. (New Riders, 2003), 186 and 222.

as TCP, UDP, and ICMP. These services allow for authentication, integrity, access control, and confidentiality. IPSec allows for encryption and verification of the information exchanged between remote sites.<sup>16</sup>

### C. WIRELESS NETWORK MANAGEMENT UTILITIES/DEVICES

Without a common wired backbone, managing wireless networks is significantly harder than managing wired networks for many reasons. One of the main problems is the unpredictable behavior of wireless channels due to fading, multi-path interference, hidden nodes, and jamming. Signal quality can vary quite dramatically, which might suddenly reduce the efficiency of the management operation. The bandwidth of wireless links is another issue that will always be limited due to the properties of the physical medium and regulatory limits on the use of radio spectrum. Therefore, it is necessary for network protocols to utilize the available bandwidth efficiently.

Wireless management interface utilities are improving but still need many changes and enhancements. Vendors are more concerned with selling low-cost wireless devices and lightweight operating systems than developing scalable and manageable enterprise-class devices. Most manufacturers save money by using low-powered hardware, which does not support the more sophisticated management interfaces. As such, SNMP-based or web-based management interfaces are what remain. Both methods have their benefits, but unless coupled with a security feature such as SSL or SNMP-v3, they are insecure.<sup>17</sup>

- **Web-based** management occurs by pointing the web browser at the access point's IP address and logging in via a username and password. The web-based network management utilities are feature-rich and easy to use.
- **Telnet** is normally accessed via wired access (i.e. serial and Ethernet). However, telnet can be enabled for wireless access as well. The implementation of **SSH** occurs rarely, but is a welcome addition to securing telnet.
- **SNMP**, as discussed earlier, is a tool (protocol) that allows for remote and local management of items on the network including servers, workstations, routers, switches and other managed devices. Most wireless devices have a SNMP agent running as a management mechanism and SNMP client software installed to access their equipment (see Figure 3.8).

---

<sup>16</sup> Kaufman, Perlman, and Speciner. *Network Security*. (Prentice Hall, 2002), 423.

<sup>17</sup> Gast. *802.11 Wireless Networks – The Definitive Guide*. (O'Reilly, 2002), 264.

- **Serial** management normally connects via a RS232 or USB connection. Most vendors will use proprietary management software for access that is capable of only running on one operating system.<sup>18</sup>

**LINKSYS**

**SETUP**

This screen contains all of the router's basic setup functions. Most users will be able to use the router's default settings without making any changes. If you require help during configuration, please see the user guide.

Host Name: C28359-A (Required by some ISPs)

Domain Name: roalok1.mi.come.com (Required by some ISPs)

Firmware Version: 1.37.1, Apr 09 2001

LAN IP Address: (MAC Address: 00-04-5A-20-1A-A1)  
 192 . 168 . 1 . 1 (Device IP Address)  
 255.255.255.0 (Subnet Mask)

WAN IP Address: (MAC Address: 00-04-5A-20-1A-A2)  
☐ Obtain an IP Address Automatically  
☒ Specify an IP Address 24 . 2 . 250 . 173  
 Subnet Mask: 255 . 255 . 252 . 0  
 Default Gateway Address: 24 . 2 . 248 . 1  
 DNS(Required) 1: 24 . 2 . 248 . 33  
 2: 24 . 2 . 248 . 34  
 3: 0 . 0 . 0 . 0

Login: ☐ PPPoE ☐ RAS ☒ Disable  
 NOTE: PPPoE is for ADSL user only.  
 RAS is for SingTel ADSL user only.

User Name:

Password:

RAS Plan: 512k Ethernet

☐ Connect on Demand: Max Idle Time 0 Min.

☐ Keep Alive

Figure 3.7. Web-Based Management Tool for Linksys WAP (From: [www.linksys.com](http://www.linksys.com), May 2004)

<sup>18</sup> Ibid.

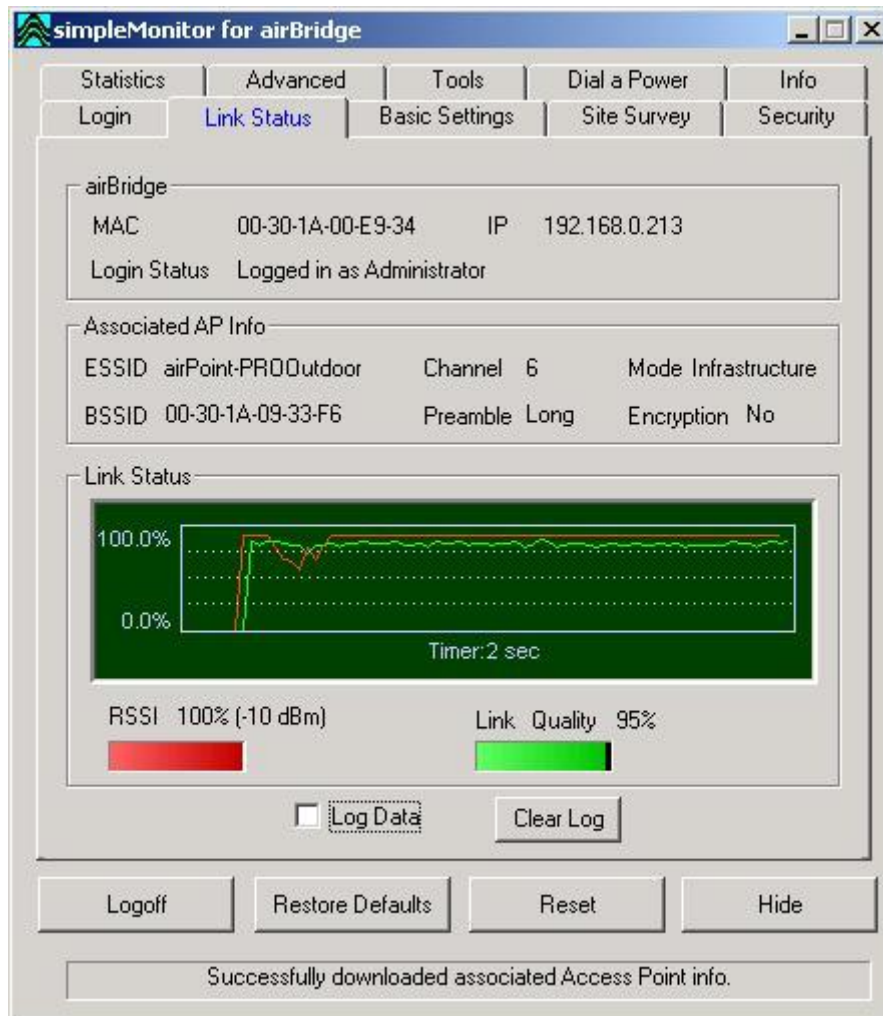


Figure 3.8. SNMP Client Software

Most enterprise wireless gateways are VPN enabled. The VPN protocols supported are most commonly PPTP, IPsec, and L2TP.<sup>19</sup>

#### D. CONCLUSION

Many different types of network management utilities exist, and each possesses advantages and disadvantages. Implementing remote management is simple. Having secure and easy to use remote management is not. This chapter provided a basic knowledge of the most common management utilities. The following chapter discusses in more detail how to implement each method in a secure fashion.

<sup>19</sup> Osbourne. *CWNA, Certified Wireless Network Administrator*. (McGraw Hill, 2003), 406.

THIS PAGE INTENTIONALLY LEFT BLANK

## IV. REMOTE NETWORK MANAGEMENT AND ITS SECURITY RISKS

### A. INTRODUCTION

The previous chapter discussed many methods for remotely managing networks. Each of these methods provides a new way for authorized remote administrators to access a system remotely but also presents a potential way for unauthorized users to gain access. The more remote utilities in use, the more ports it is necessary to open in the perimeter firewall, thereby weakening defenses.

This chapter discusses some methods for reducing the risk of using remote management utilities. It is important to understand that the fewer utilities used the better. Limiting the amount of remote network utilities not only limits the amount of holes in the perimeter defenses, but it is easier for the remote network administrator to manage since fewer utilities exist with which to interface.

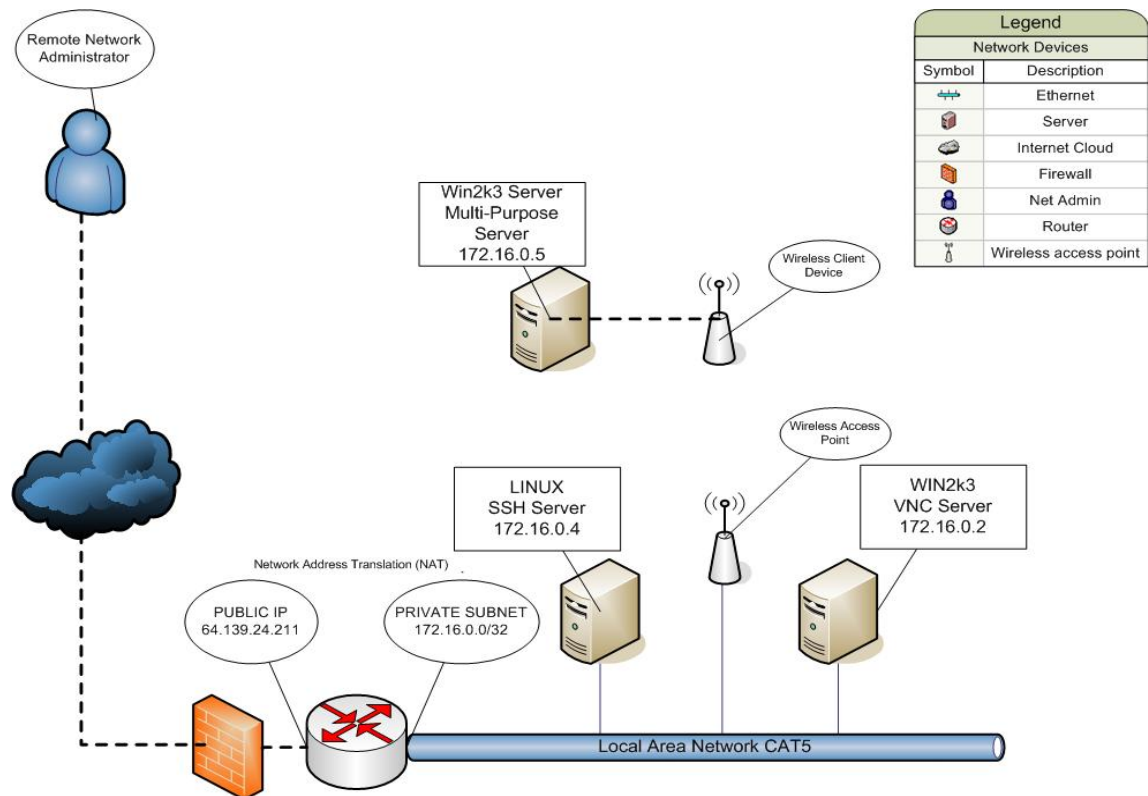


Figure 4.1. Test-Bed Network developed for thesis testing

## B. WIRED NETWORK REMOTE MANAGEMENT UTILITIES

Wired network remote management utilities include Telnet, SSH, SNMP, Remote Desktop Utilities, and Virtual Private Networks (VPN's). Each of these utilities has its pros and cons based on functionality and security. This section will discuss how to utilize each of the utilities effectively and securely.

### 1. Telnet

**Telnet** passes login name and password in clear text, yet it remains the most popular method of remotely administering network devices. It is possible to configure any basic network sniffer, such as Ethereal (www.Ethereal.com), to watch for telnet traffic on the network. For this reason, capturing and exploiting usernames and passwords is easy when using telnet. Figure 4.1 shows password “cisco” in clear text.<sup>20</sup>

No.	Status	Source Address	Dest Address	Summary	Len	Rel. Time
32		[192.168.1.5]	[192.168.1.50]	Telnet: R PORT=1904 r	64	0:00:18
33		[192.168.1.5]	[192.168.1.50]	Telnet: R PORT=1904 u	64	0:00:18
34		[192.168.1.5]	[192.168.1.50]	Telnet: R PORT=1904 n	64	0:00:18
35		[192.168.1.5]	[192.168.1.50]	Telnet: R PORT=1904 <0D0A>	64	0:00:18
36		[192.168.1.5]	[192.168.1.50]	Telnet: R PORT=1904 Building conf	81	0:00:18
37		[192.168.1.5]	[192.168.1.50]	Telnet: R PORT=1904 <0D0A>Current	527	0:00:19
38		[192.168.1.5]	[192.168.1.50]	Telnet: R PORT=1904 <080808080808	530	0:00:21
39		[192.168.1.5]	[192.168.1.50]	Telnet: R PORT=1904 <080808080808	462	0:00:21
40		[192.168.1.5]	[192.168.1.50]	Telnet: R PORT=1904 <080808080808	449	0:00:22
41		[192.168.1.5]	[192.168.1.50]	Telnet: R PORT=1904	64	0:00:22
00000120:		72 20 74 72 61 70 2d 61 75 74 68 65 6e 74 69 63		r trap-authentic		
00000130:		61 74 69 6f 6e 0d 0a 73 6e 6d 70 2d 73 65 72 76		ation..snap-serv		
00000140:		65 72 20 63 68 61 73 73 69 73 2d 69 64 20 30 78		er chassis-id 0x		
00000150:		30 45 0d 0a 21 0d 0a 6c 69 6e 65 20 63 6f 6e 20		0E...line con		
00000160:		30 0d 0a 20 70 61 73 73 77 6f 72 64 20 63 69 73		0.. password cis		
00000170:		63 6f 0d 0a 20 6c 6f 67 69 6e 0d 0a 20 73 74 6f		co.. login.. sto		
00000180:		70 62 69 74 73 20 31 0d 0a 6c 69 6e 65 20 76 74		pbits 1..line vt		
00000190:		79 20 30 20 34 0d 0a 20 70 61 73 73 77 6f 72 64		y 0 4.. password		
000001a0:		20 63 69 73 63 6f 0d 0a 20 6c 6f 67 69 6e 0d 0a		cisco.. login..		
000001b0:		21 0d 0a 65 6e 64 0d 0a 0d 0a 53 77 69 74 63 68		!..end....Switch		
000001c0:		23		#		

Figure 4.2. Telnet Login Password (Cisco) Shown in cleartext (From: [www.ethereal.com](http://www.ethereal.com), May 2004).

<sup>20</sup> Northcutt, Zeltser, Winters, Frederick, and Ritchey. Inside Network Perimeter Security. New Riders, 2003, 144.



Using access control lists and limiting the telnet access to only those authorized to administer the network device can make telnet more secure. Furthermore, the use of network switches in lieu of hubs will limit the interception location of telnet traffic. For these reasons, telnet should be disabled and blocked at the perimeter firewall unless it is the only method of administration.<sup>21</sup>

## 2. SSH

**SSH** is the secure substitute for telnet. SSH uses public key-based authentication or strong encryption to protect the username and password during the authentication process. This prevents network sniffers from capturing the login information.<sup>22</sup> It is necessary to always verify the SSH server's fingerprint when establishing the SSH connection for the first time. (see Figure 4.2).

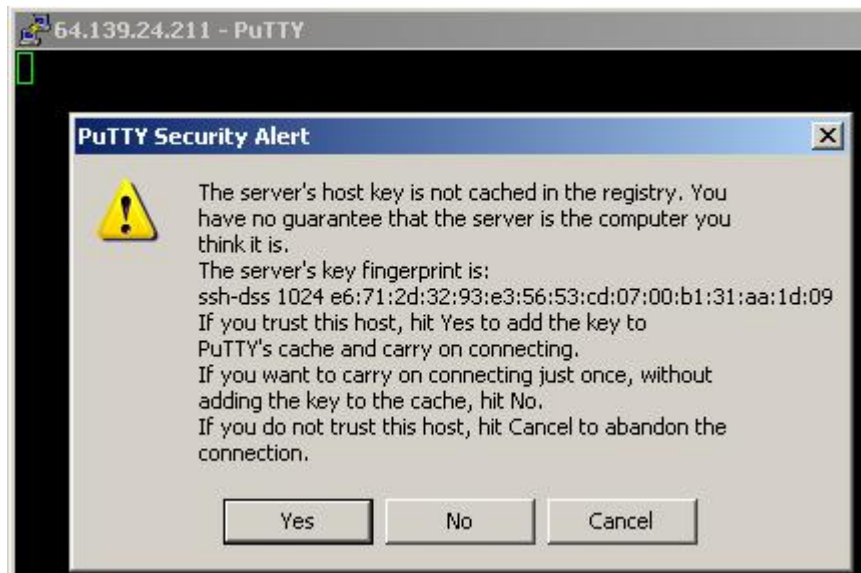


Figure 4.3. Initial SSH Connection Shows Server Fingerprint

Most manufactures still use cleartext telnet for remote command-line interfaces, although it is possible to license OpenSSH for incorporation into proprietary products at no charge ([www.openssh.com](http://www.openssh.com)).

<sup>21</sup> Barnes, Bautts, Lloyd, Ouellet, Posluns, Zendzian. Hack Proofing your Wireless Network. Syngress, 2002,78.

<sup>22</sup> Northcutt, Zeltser, Winters, Frederick, and Ritchey. Inside Network Perimeter Security. New Riders, 2003, 145.

### 3. SNMP

**SNMP** is an easy and popular way of managing network devices, especially in large, complicated networks. However, versions 1 and 2c, like telnet, pass login information in the form of community strings (also known as passwords) in the clear (see Figure 4.1). SNMP version 3 supports encryption and cryptographic authentication. Therefore, if SNMP is required for remote network management, SNMP version 3 is highly recommended.<sup>23</sup> Once again, it is highly recommended to disable SNMP management and block it at the perimeter firewall unless it is the only method of management available.

### 4. Remote Desktop Utilities

**Remote Desktop utilities**, without the use of encryption, are wide-open to “man-in-the-middle” attacks. Not only is the login information normally sent in the clear, a “man-in-the-middle” could easily view the exact desktop at the same instant the remote administrator is viewing it. The following remote desktop utilities have incorporated, at a minimum, login encryption.

#### a. *Windows Remote Desktop Protocol*

Windows Remote Desktop Protocol (RDP) now incorporates RSA Security's RC4 cipher for security. Beginning with Windows 2000, administrators can choose to encrypt data using a 56- or 128-bit key. To prevent unauthorized interception of the data as it travels between the client and server, enable encryption. This capability prevents sending login information in the clear, and therefore, is significantly more secure.

Encryption can be set to one of the following three levels:<sup>24</sup>

- High: encrypts both the data sent from client to server and the data sent from server to client using a 128-bit key.
- Medium: encrypts both the data sent from client to server and the data sent from server to client using a 56-bit key if the client is a Windows 2000 or above client, or a 40-bit key if the client is an earlier version.

---

<sup>23</sup> Barnes, Bautts, Lloyd, Ouellet, Posluns, Zendzian. Hack Proofing your Wireless Network. Syngress, 2002, 315.

<sup>24</sup> <http://www.microsoft.com/windowsxp/remotedesktop/>. March, 2003.

- Low: encrypts only the data sent from client to server, using either a 56 or 40-bit key, depending on the client version. Useful to protect usernames and passwords sent from client to server.

RDP also incorporates various levels of data compression and caching to reduce the amount of transmitted data. This greatly enhances the performance over low-bandwidth connections.

#### ***b. Virtual Network Computing (VNC)***

Virtual Network Computing (VNC) has little security built-in. It provides encrypted username password authentication, but no encryption for the data that follows. Therefore, tunneling VNC over Secure Shell is critical. It is first necessary to setup the VNC server to listen on an obscure port such as port 6005. The VNC server is defaulted to listen on port 5900, but default settings are rarely acceptable from a security standpoint, as discussed later in this chapter. To change the listening port from 5900 to 6005, add 105 in the Display Number block (see Figure 4.4). Then, check the Accept Socket connections and enter a difficult password following DoD password guidelines. To improve network performance, it is also a good idea to remove the desktop wallpaper.

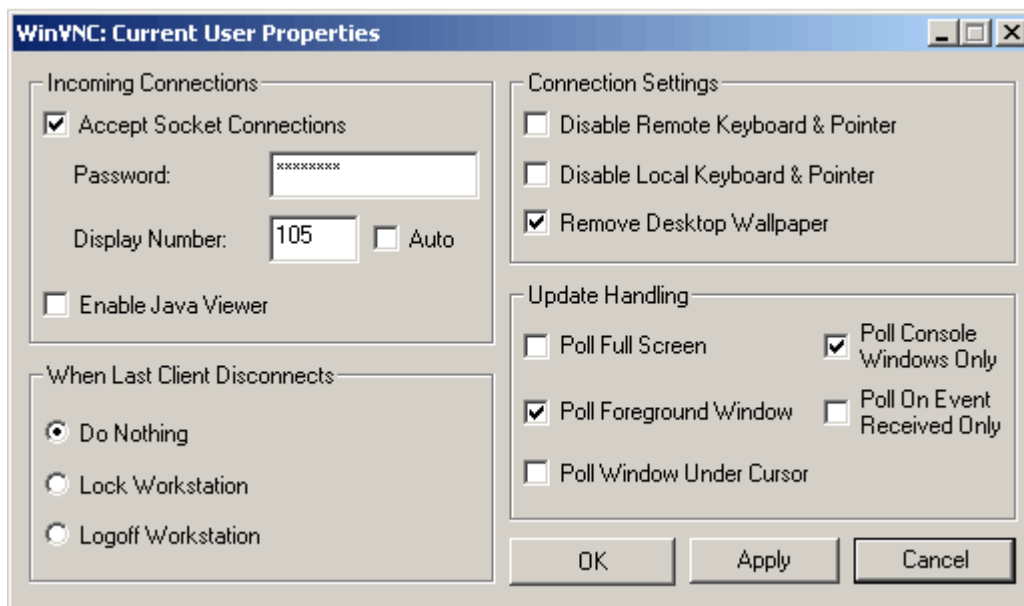


Figure 4.4. VNC Server Configuration

The next step is to setup the SSH tunnel. Using PuTTY, a freeware SSH client for both Windows and Unix platforms, with port forwarding is relatively simple. The first step is to setup the connection within PuTTY (see Figure 4.5).

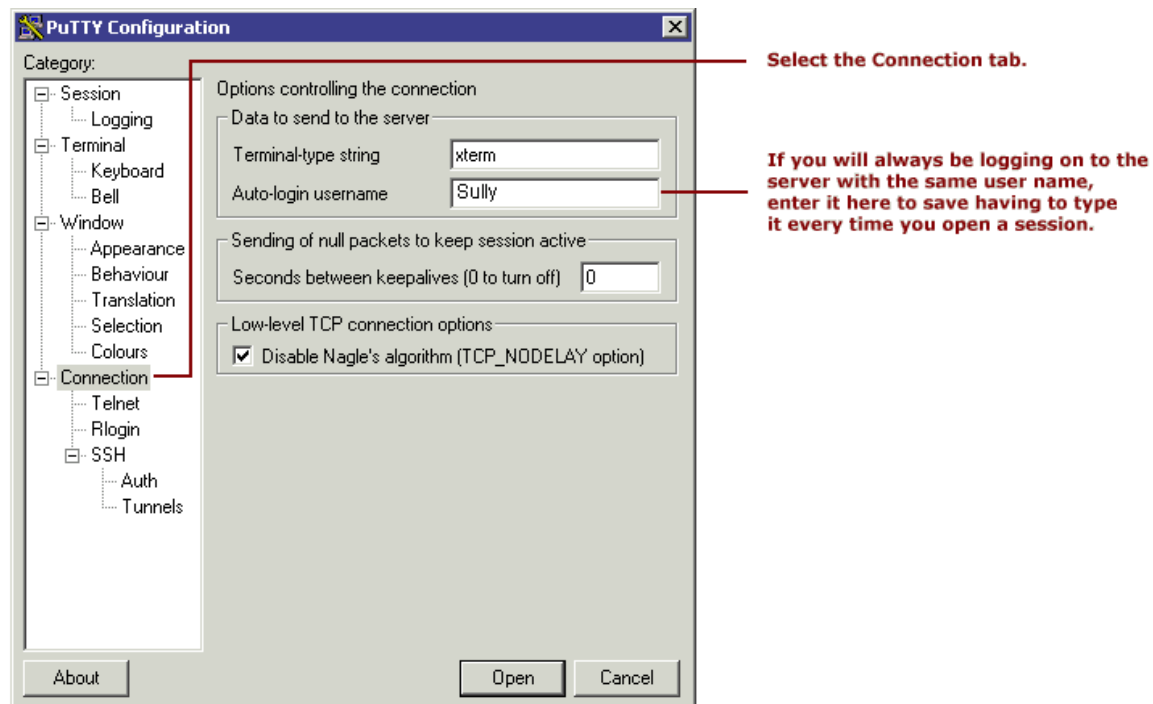


Figure 4.5. PuTTY Connections

The next step is to setup the appropriate SSH version and compression (see Figure 4.6). By enabling compression, VNC will perform much better over low-bandwidth connections.

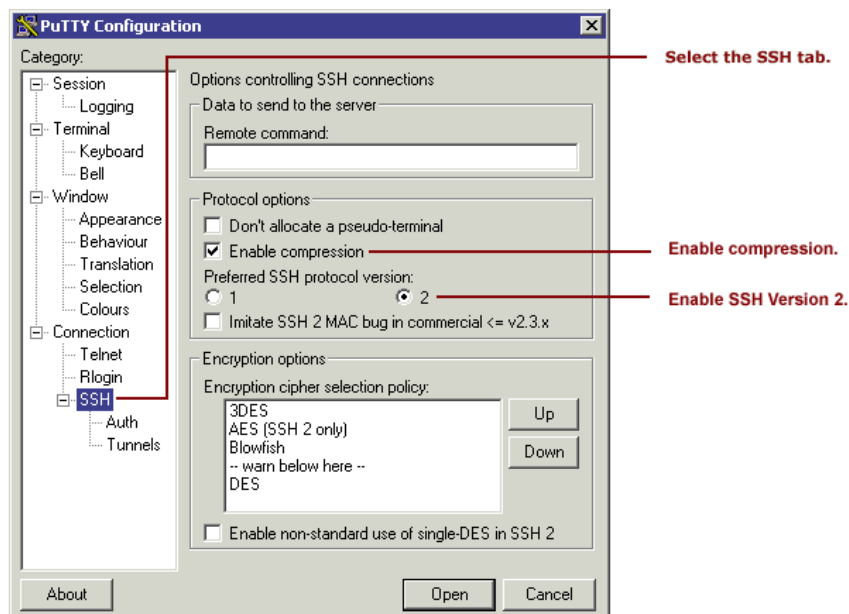


Figure 4.6. PuTTY SSH Version and Compression

As stated earlier, VNC by default is listening on port 5900. Therefore, it is necessary to forward localhost port 5900 requests down the SSH tunnel to the remote machine (172.16.0.2) which is listening on port 6005 (see Figure 4.6).

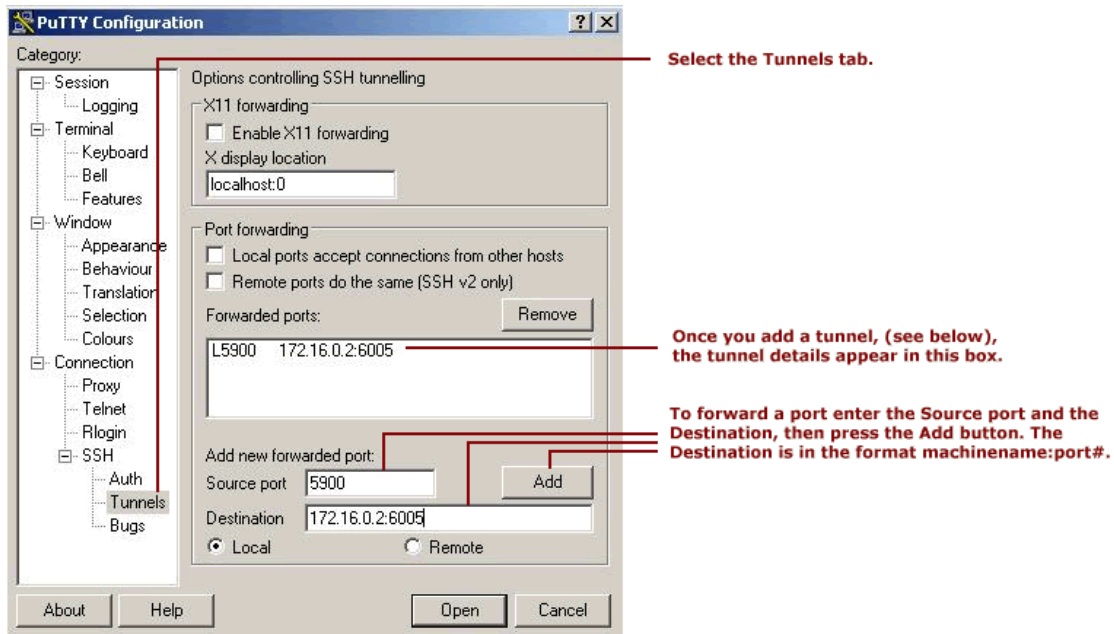


Figure 4.7. PuTTY Tunnel Configuration

Finally, it is possible to enter the remote SSH server's IP address, select SSH, and name the connection for future use (see Figure 4.7).

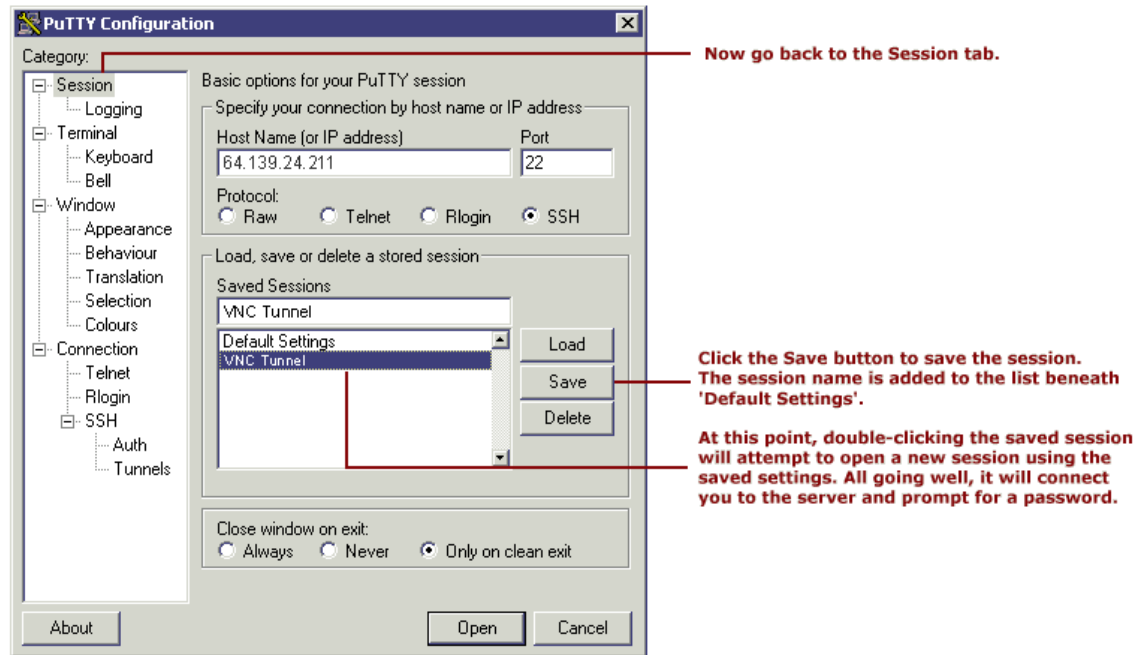


Figure 4.8. PuTTY Session Configuration

Once the SSH connection is made, the localhost (127.0.0.1) is connected to via the VNC client which will be forwarded down the encrypted tunnel to the remote VNC server (see Figure 4.9). Thus, the entire VNC session is now fully encrypted.

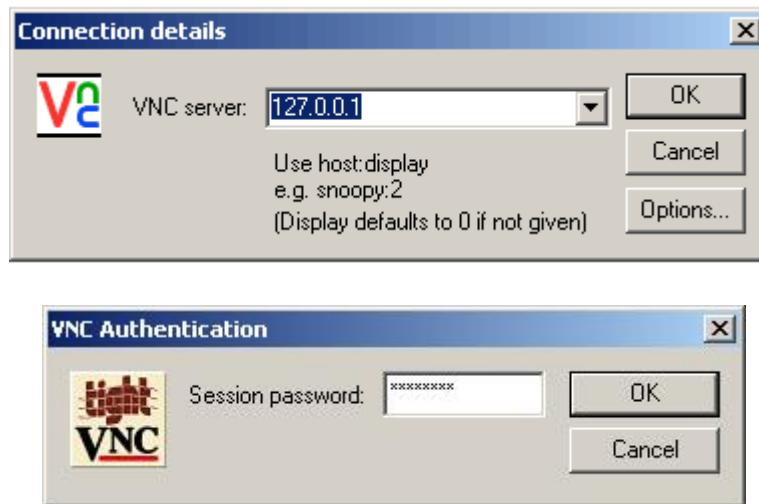


Figure 4.9. VNC Remote Login through SSH Tunnel

### c. Citrix

Citrix MetaFrame Access Suite along with the Citrix ICA client software is a better solution than VNC for the corporate network. It is possible to configure the

Citrix MetaFrame Server to accept only SSL and/or 128-bit connections from its remote clients, thereby, securing not only the authentication process, but all the data following login. Clients configuring the Citrix ICA client should enable 128-bit encryption (see Figure 4.10).

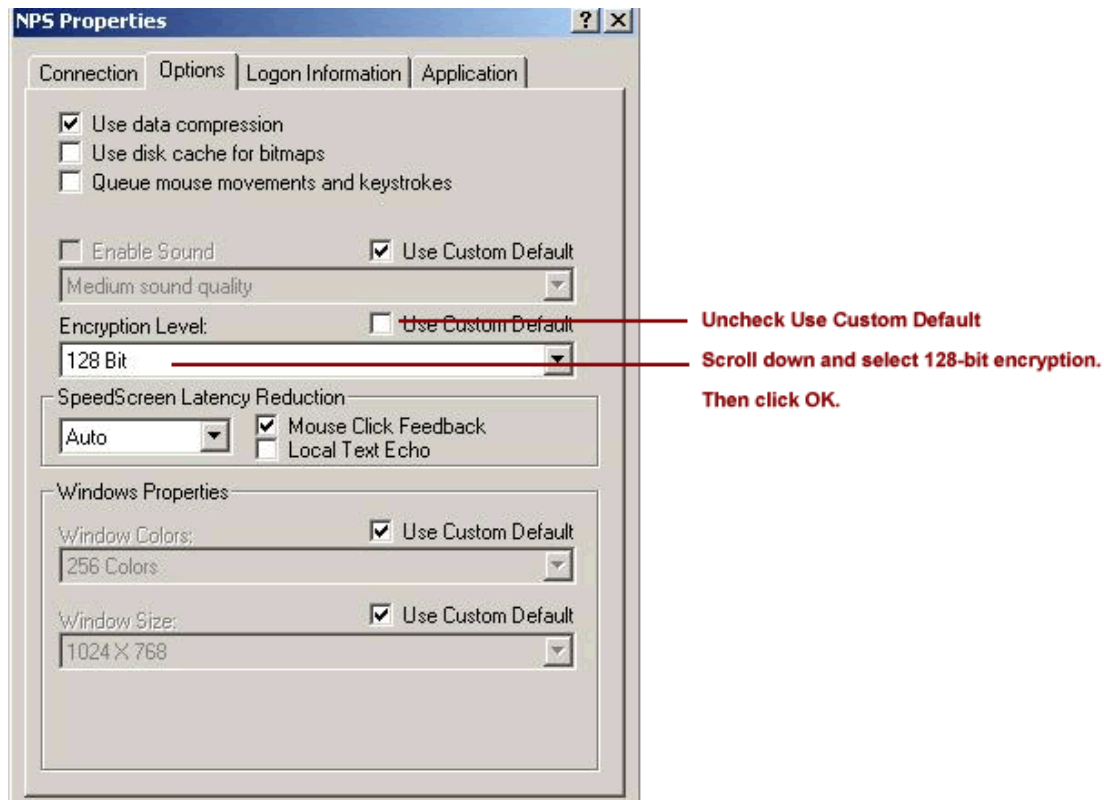


Figure 4.10. Citrix ICA 128-bit Encryption Configuration

#### ***d. GoToMyPC***

GoToMyPC Corporate and GoToMyPC Personal edition are two entirely different software versions. The individual subscriber uses the GoToMyPC Personal edition while the GoToMyPC Corporate edition is for secure remote access to businesses. The GoToMyPC Corporate platform comes with an online Administration Center and reporting features that help clients manage remote access to employees. Both products use AES with 128-bit keys to protect the data stream, file transfers, and other input. The platforms also offer other built-in security features such as dual passwords, user authentication, host screen blanking and host keyboard and mouse locking.<sup>25</sup>

<sup>25</sup> [www.GoToMyPC.com](http://www.GoToMyPC.com). (March, 2004).

Individual computers have the GoToMyPC Personal edition software installed that is capable of circumventing corporate or personal firewall rules. This host software communicates with the GoToMyPC servers every 15 seconds via http port 80, and thus, the host is opening an outbound communications channel through the firewall. Since the host initiates all of the communications, it can penetrate firewalls and NAT devices. The GoToMyPC servers relay messages between the web client and the host allowing remote access to the computer by simply logging onto GoToMyPC.com's webpage and selecting the appropriate host machine. This process circumvents corporate policy and creates a weak link in the firewall.

GoToMyPC will work in most cases without any reconfiguration of the firewall. GoToMyPC hosts first try to contact the broker server over TCP port 8200. If that fails, the broker server receives the HTTP GET requests on port 80 (see Figure 4.11.). The connection will succeed with permitted web browsing. Blocking the GoToMyPC Personal edition requires blocking access to the broker server “poll.gotomypc.com” within the firewall filters. This will not allow the host software to initiate the outbound connection with GoToMyPC servers, thereby eliminating the capability for remote management.

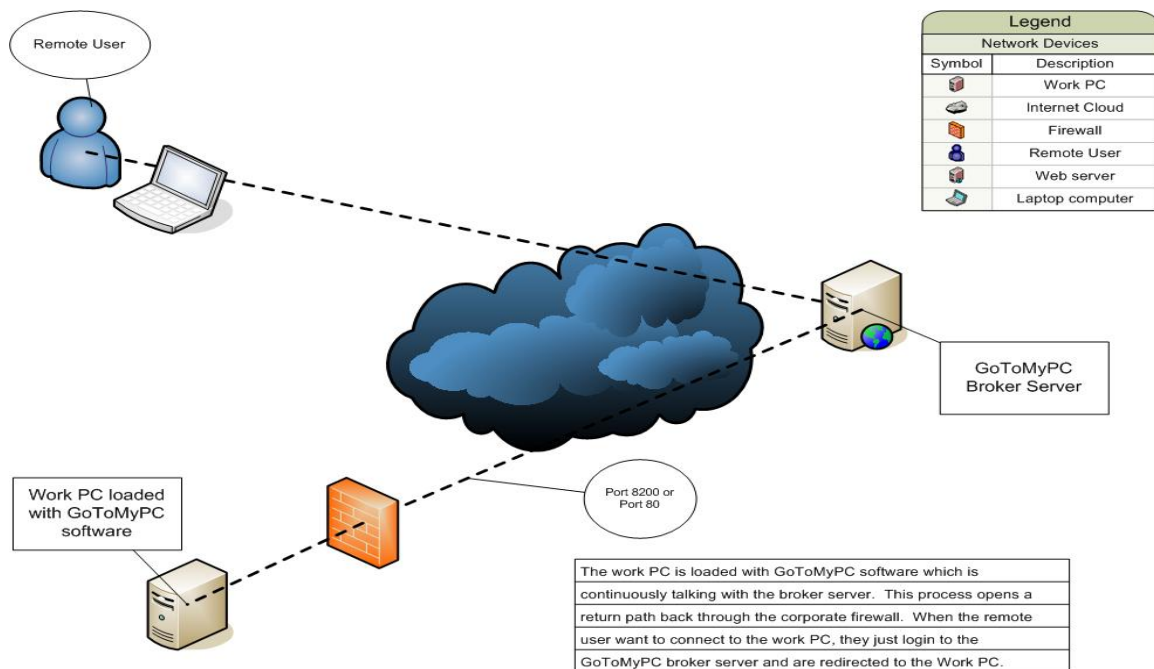


Figure 4.11. GoToMyPC circumvents firewall policies.



The GoToMyPC Corporate Edition, like the Personal edition, allows users to access their computers remotely via the Internet. However, the Corporate Edition is a more secure solution due to its complete online administration center that allows the remote administrator total control over remote access. GoToMyPC Corporate also incorporates SSL log-in, nested passwords, end-to-end 128-bit Advanced Encryption Standard (AES) encryption, and authentication.<sup>26</sup>

## **5. VPN**

**Virtual Private Networks (VPNs)** are the best solution available today for connecting disconnected networks over a public medium, while maintaining confidentiality, data integrity, and authentication. With VPN clients becoming a mainstream component in most operating systems, the disadvantages of implementing VPNs are nearly nonexistent. The comparison of each of the following VPN solutions shows a few advantages over the other.<sup>27</sup>

### ***a. Point-to-Point Tunneling Protocol (PPTP)***

**Point-to-Point Tunneling Protocol (PPTP)** provides a Generic Record Encapsulation of PPP (including LCP frames). It allows PPP to be routed. PPTP by itself specifies no message integrity or privacy. Unlike IPsec, it is protected in practice by Microsoft's implementation of PPTP which uses Microsoft's MPPE Protocol. Many hardware devices and operating systems also integrate with PPTP making it available. One disadvantage of PPTP is its vulnerability to man-in-the-middle attacks due to the lack of server authentication.

### ***b. Layer 2 Tunneling Protocol***

**L2TP** is the combination of Cisco's Layer Two Forwarding (L2F) protocol and PPTP. L2TP uses UDP, a connectionless protocol, for all its packets thereby reducing overhead. L2TP can also create multiple tunnels between hosts, which PPTP and IPsec cannot. (PPTP allows multiple tunnels, one from each client to a single PPTP server). L2TP by itself does not provide message integrity or confidentiality. In order to do the latter, it is necessary to combine it with IPsec.

---

<sup>26</sup> Ibid.

<sup>27</sup> Northcutt, Zeltser, Winters, Frederick, and Ritchey. Inside Network Perimeter Security. New Riders, 2003, 222.

*c. Internet Protocol Security*

**IPSec** is the only protocol that is an IETF standard. IPSec can protect any protocol that runs on top of IP, whereas PPTP and L2TP also support non-IP protocols. The IPSec protocols (AH and ESP) can be used to protect either an entire IP payload (Tunneling Mode) or only the upper-layer protocols of an IP payload (Transport Mode). NAT can break IPSec since authentication data may be computed over a source IP address.

*d. L2TP + IPSec*

**L2TP + IPSec** is better than PPTP. . L2TP over IPSec is a Microsoft encapsulation found in Microsoft's Windows Server. Advantages of L2TP/IPSec over PPTP include server authentication, data integrity, two levels of authentication, and confidentiality. The use of machine certificates for machine-level authentication of VPN clients and VPN server is required for L2TP over IPSec-based VPN connections. This provides both computer and user authentication.

In order to create an L2TP over IPSec connection, it is necessary to install a machine certificate, also known as a computer certificate, on the VPN client and VPN server computer. The network administrator or network security specialist will maintain the certificate authority and the issuance of certificates. Depending on the level of security required, the certificate authority can issue certificates via the web or in person only. Man-in-the-middle attacks are not possible because if any of the information moving through the tunnel changes while in transit, the receiving L2TP/IPSec VPN server will drop the packets.<sup>28</sup>

*e. Tunneling*

**Tunneling** is defined as "a technology that enables one network to send its data via another network's connections. Tunneling works by encapsulating a network protocol within packets carried by the second network." Microsoft's PPTP technology performs this by embedding its own network protocol within the TCP/IP packets carried by the Internet. Tunneling and encapsulation are synonymous.<sup>29</sup>

---

<sup>28</sup> Ibid., 223.

<sup>29</sup> <http://www.webopedia.com>. (March 2004).

One of the easiest forms of tunneling is via SSH (see Figure 4.7). An SSH tunnel can be setup for almost any traffic via port forwarding. SSH tunneling is a cost effective method of allowing remote users to use insecure protocols over public networks. SSH tunneling can also be setup extremely quickly and inexpensively compared to other VPN solutions.<sup>30</sup>

### **C. WIRELESS NETWORK REMOTE MANAGEMENT UTILITIES**

Due to the increasing popularity of wireless products, manufacturers have made it easy to roll out wireless connectivity. Thus, most manufacturers configure default settings with ease in mind, not security. Therefore, it is imperative for the wireless network administrator to spend time changing the default settings to the highest security level possible, prior to roll out. In other words, the administrator should make the wireless network as easy as possible for users while not sacrificing overall security.

It is important to not treat the wireless access points differently from Remote Access Servers, and place them outside the network firewalls or within the DMZ. Running the wired backbone of the wireless access points on a separate virtual LAN (VLAN) is highly recommended. This will allow the implementation of a wireless authentication firewall such as Cranite Systems' access controller ([www.cranite.com](http://www.cranite.com)) for added security (see Figure 4.11).<sup>31</sup>

---

<sup>30</sup> Northcutt, Zeltser, Winters, Frederick, and Ritchey. Inside Network Perimeter Security. New Riders, 2003, 384.

<sup>31</sup> Barnes, Bautts, Lloyd, Ouellet, Posluns, Zendzian. Hack Proofing your Wireless Network. Syngress, 2002, 315.

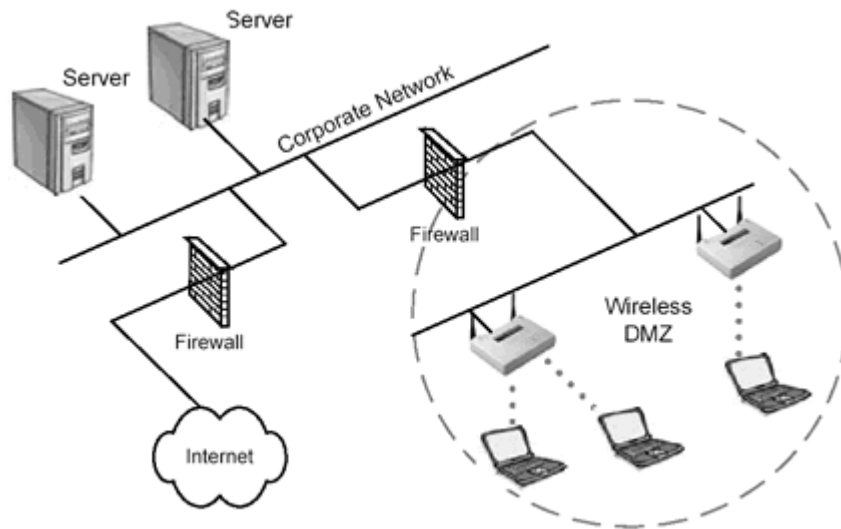


Figure 4.12. Wireless Access Points in DMZ (From: Osbourne. CWNA, Certified Wireless Network Administrator. McGraw Hill, 2003, 418)

When wireless devices are implemented in a campus or corporate setting, each of the wireless devices will normally share a common wired backbone (see Figure 4.11). For this reason, management of the wireless devices does not require wireless remote management, and is therefore, no different from wired remote management as previously discussed.

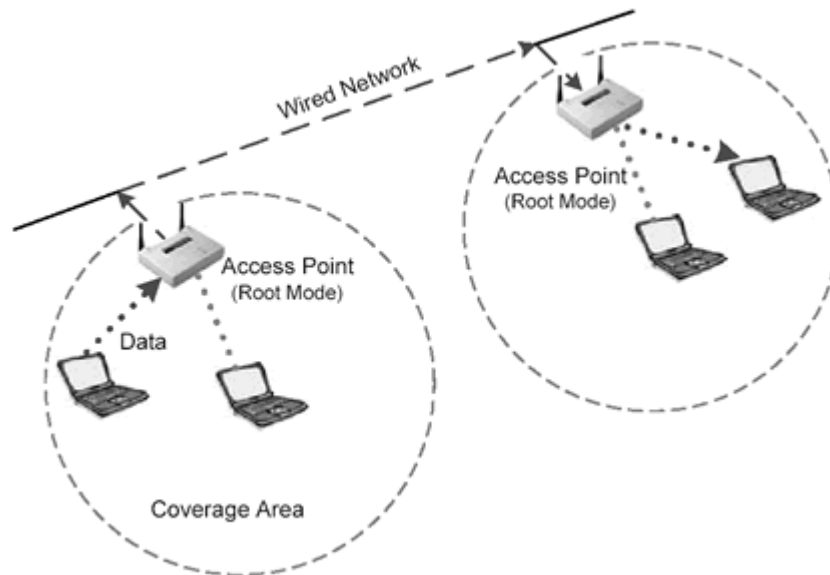


Figure 4.13. Common Wired Backbone (From: Osbourne. CWNA, Certified Wireless Network Administrator. McGraw Hill, 2003, 101)

If wireless management is required, such as with a wireless bridge (see Figure 4.12), it is imperative to consider wireless network management interfaces when procuring new equipment. The access of the Wireless access points occurs from the wired side or across the wireless signal itself when using a wireless bridge. The recommendation is to use the wired side whenever possible for performing management. The following section discusses various methods of wireless remote management with emphasis on security.<sup>32</sup>

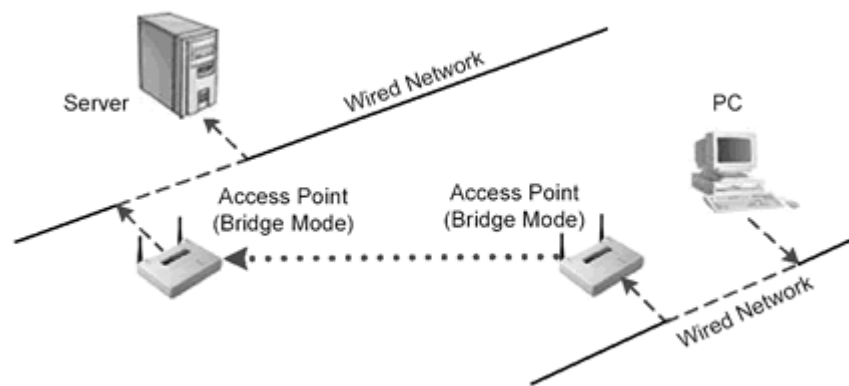


Figure 4.14. Wireless Bridge (From: Osbourne. CWNA, Certified Wireless Network Administrator. McGraw Hill, 2003, 102)

**Web-based** remote management, although intuitive and feature rich, is also insecure. Without implementing SSL, web-based management is in the clear and easily intercepted. If SSL is not available, and web-based management is the only method, tunneling over the public domain via SSH is highly recommended. By tunneling over the public domain, only the trusted internal network will see the web-based management traffic.

**Telnet** management, like web-based management, is insecure. Disabling it is a serious consideration. Telnet management is common on older wireless products but is being phased out by SSH implementation. If Telnet is the only method of management, it is necessary to use SSH tunneling across untrusted domains.

---

<sup>32</sup> Osbourne. CWNA, Certified Wireless Network Administrator. McGraw Hill, 2003, 129.

**SNMP** version 3 is the only secure SNMP version available today. SNMP versions 1 and 2c both use cleartext community strings (passwords). SNMP version 3 uses encryption to protect the community string and data. With all versions of SNMP, administrators should change all default community strings immediately. In most cases, the default community strings are *public* and *private*.<sup>33</sup>

**SSH** is by far the most common *secure* management method available today. Manufacturers of enterprise-class wireless devices are realizing the importance of security and are now implementing SSH in place of other wireless management methods. SSH is highly recommended as a replacement for Telnet, web-based, and SNMP management.

**Serial** management is secure since a single direct cable connects the wireless device and management PC. Since this cable is not shared across the network, it is, therefore, free from eavesdroppers. Although serial management is secure, it is not practical after the deployment of the wireless access points in their remote locations.

**VPN** servers are available with some high-end wireless devices. Not only is it possible to use the VPN server for remote management, but it can also encrypt all user data between associated client devices. This method is secure but has high overhead because of the incorporation of the VPN server within the access point.<sup>34</sup>

**EAP-TLS (Transport Layer Security)** provides for certificate-based and mutual authentication of the client and the network. This method is by far the most secure available. It relies on client-side and server-side certificates to perform authentication and another possibility is to use it to generate user-based and session-based WEP keys dynamically to secure subsequent communications between the WLAN client and the access point.<sup>35</sup>

One drawback of EAP-TLS is that certificates must be managed on both the client and server side. Since the creation of a PKI infrastructure is already occurring within DoD, instituting EAP-TLS would not be difficult. By utilizing a strict certificate

---

<sup>33</sup> Northcutt, Zeltser, Winters, Frederick, and Ritchey. Inside Network Perimeter Security. New Riders, 2003, 245.

<sup>34</sup> Osbourne. CWNA, Certified Wireless Network Administrator. McGraw Hill, 2003, 128.

<sup>35</sup> RFC 2716.

issuance policy, all wireless devices connected to a corporate backbone will have certificates issued in person.

#### **D. CONCLUSION**

The deployment of wired and wireless networks within the Department of Defense requires that security be the number one concern when designing the remote management platform. It is necessary to consider the risk verses cost ratio when deciding on the level of security implementation. The higher the level of security, the higher the associated costs.

As discussed in this chapter, many methods exist to manage both wired and wireless networks. However, it is imperative that some methods are not used, such as Telnet and SNMP v1, unless necessary. Transmitting passwords in the clear is never a good idea, especially when managing a mission-essential piece of network equipment.

Managing network devices over an untrusted network, like the Internet, can be just as secure as managing network devices on a trusted LAN if the right utilities are used and used correctly. At a minimum, all tunneled over the unsecure network via SSH. VPN technology, while very secure and functional, is sometimes cost prohibitive depending on the size of the network being managed. Another factor that greatly affects which remote management utility is used, is the mobility of the network itself. In some cases, the network being managed may be a tactically deployed unit that is constantly on the move.

Wireless networks can be operated and managed securely with the use of EAP-TLS. EAP-TLS enabled wireless devices are costly, but well worth the added cost. Basic Wired Equivalent Privacy (WEP) has been widely advertised as defective. The Department of Defense should never use WEP as its sole wireless security measure, nor should it use TKIP.

In order to determine the functionality, security, and overall effectiveness of network management utilities, a test-bed network was built, which consisted of an enterprise class router, firewall, five servers, two wireless access points, three wireless client devices, one network switch, and several desktop PCs. This test bed was administered over several months utilizing the aforementioned network management

utilities. Remote power management was determined to be a weak link, due to several instances in which network equipment had locked up, causing a power reset at the remote location. The following chapter discusses remote power management.



## **V. DEVICES LACKING NETWORK MANAGEMENT (OR THE WEAK LINK)**

### **A. INTRODUCTION**

The aforementioned network management utilities are not always useful if the device in question is not network addressable or is locked up. Managing power control devices remotely, such as Uninterruptible Power Supplies (UPSs), is just as important as having remote management capability for servers. It is easy to find these devices on the websites of some of the major manufacturers such as American Power Conversion (APC) <http://www.apc.com> or Minuteman UPS <http://www.minutemanups.com>. However, having an IP-addressable UPS may not be enough, for example when a key router locks up. What is necessary to manage the UPS or any other network device remotely if the point-of-entry router is down? For this reason, backup methods must exist to perform a hard power reset of the associated device.

Months were spent testing and building different power management devices. These devices provide not only remote management abilities, but also have back-up methods for management, incorporating also some automatic features that enable the power management device to reboot locked up equipment without technician response. The evolutionary phases of this test bed, as well as the needs driving the effort, are explained in great detail within this chapter.

### **B. TAKING CONTROL OF YOUR POWER**

In order to have complete remote management, all pieces of the network puzzle must have remote management capability; and the more automatic the better. The installation of an automatic method of remote power management not only reduces downtime but also eliminates the associated man-hours involved with rebooting the hardware. Consider the following scenarios in order to understand the need for remotely manageable power devices.

The Department of Defense continuously strives to do more with less. In this endeavor, more locations are becoming unmanned or experiencing reduced manning by taking advantage of remote management capability. Remotely managing a server has become simple and secure using the tools outlined in the previous chapters. However,

the question remains of how to manage a completely locked up server. Is the solution to send a technician, possibly hours away, to the remote location just to reboot the locked device? The answer is simple: use remotely manageable UPSs that incorporate several methods of remote management, as well as automatic reboot technology when available.

Recent advances in backup power supplies have included built-in processors providing special management features such as the monitoring of power consumption, load percentage, and temperatures. Some UPSs also have the ability to reboot locked-up hardware remotely by logging into the UPS via the Internet and choosing the appropriate device for reboot (see Figure 5.1).

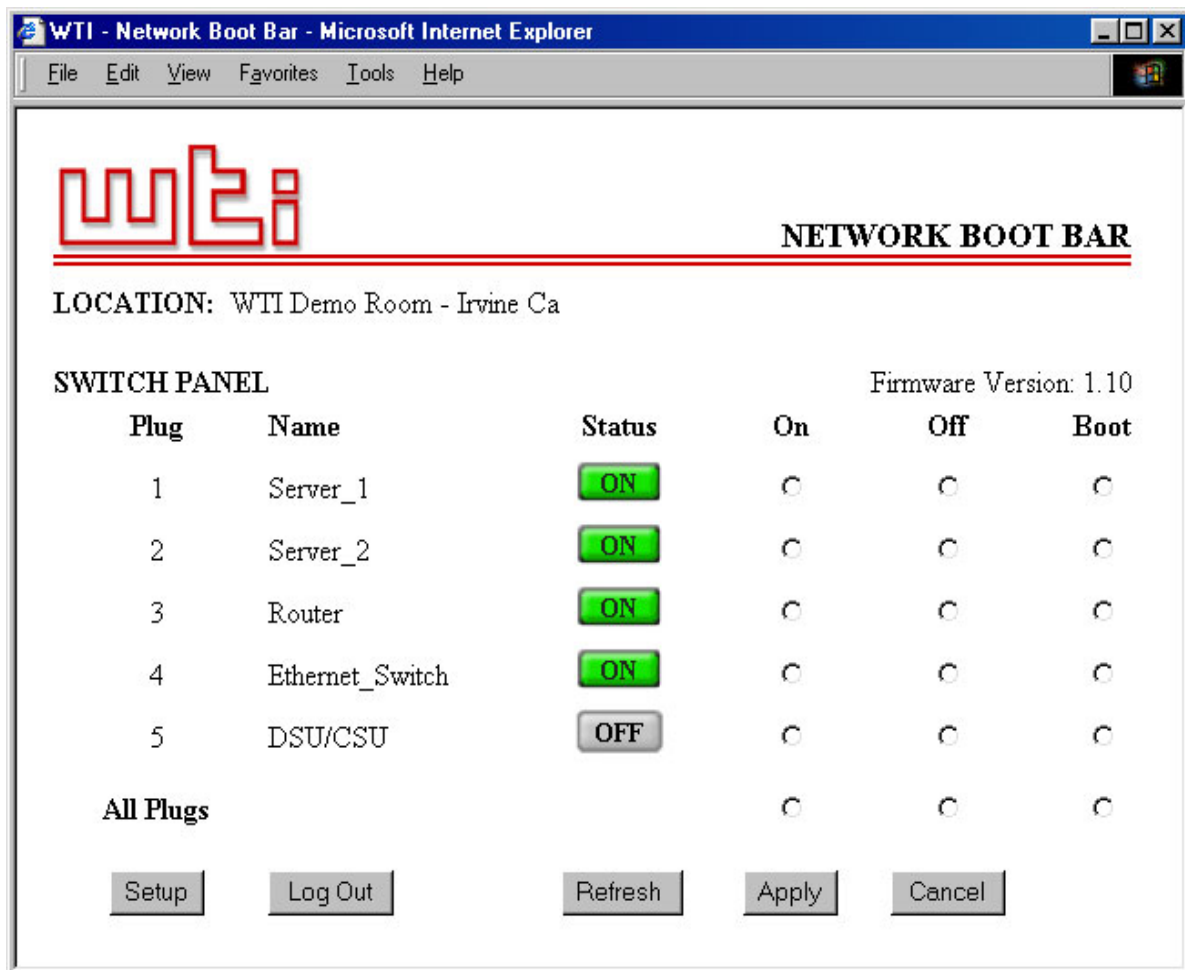


Figure 5.1. Web-Based Interface Rebooter (From: <http://www.wti.com>, May 2004)

Finding an UPS, which is manageable via IP, is simple. However, IP cannot be the only means of remotely managing a network. If the point-of-entry router locks up, a

technician must deploy to the remote location to reboot the associated device (see Figure 5.2). Therefore, it is necessary to have backup methods to minimize an on-site technician response. Several backup methods are currently available, including dial-up modems, telephone touch-tone controllers, and auto watchdog capabilities.

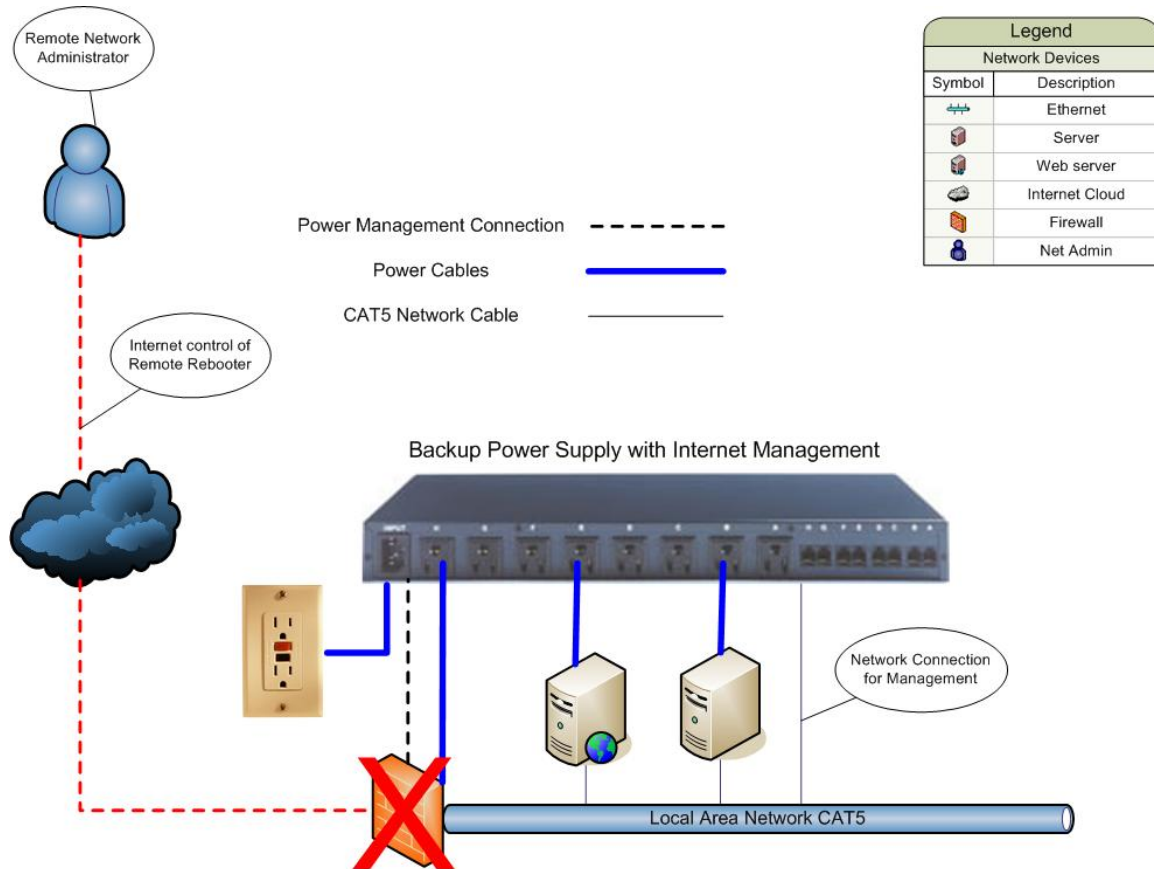


Figure 5.2. Remotely Manageable UPS is Unreachable Due to Key Router Being Down

### C. BACKUP METHODS OF REMOTE POWER REBOOTING

A UPS can be purchased with a preinstalled modem for dial-up telnet or SSH. This would allow the remote network administrator to dial-in and initiate a hard power-reset of the locked-up device, eliminating the need for a costly technician rollout (see Figure 5.3).

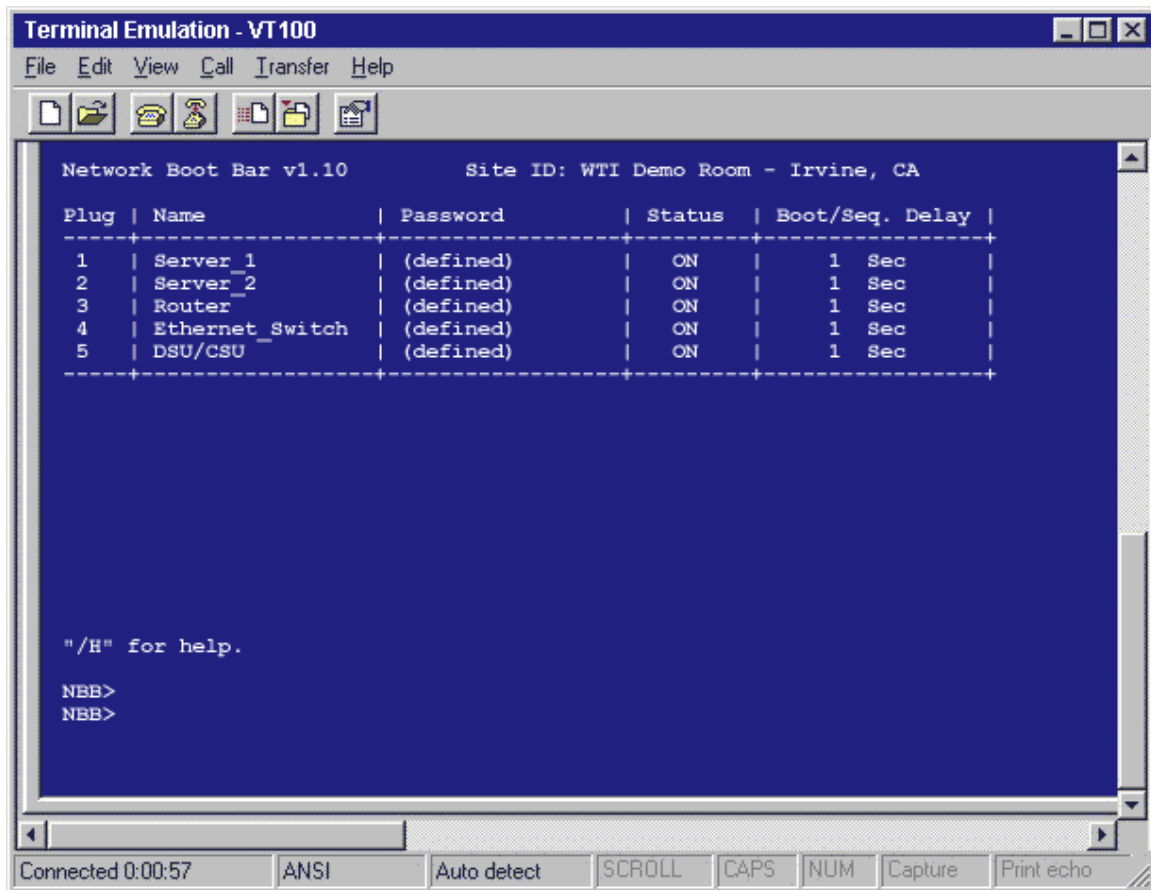


Figure 5.3. Command Line Interface for Remote Rebooter (From: <http://www.wti.com>, May 2004)

This method requires a modem and a dedicated modem line for each UPS at the remote location, which can be costly, in addition to a phone line at the administrator's location, and remote administrator assistance (see Figure 5.4).

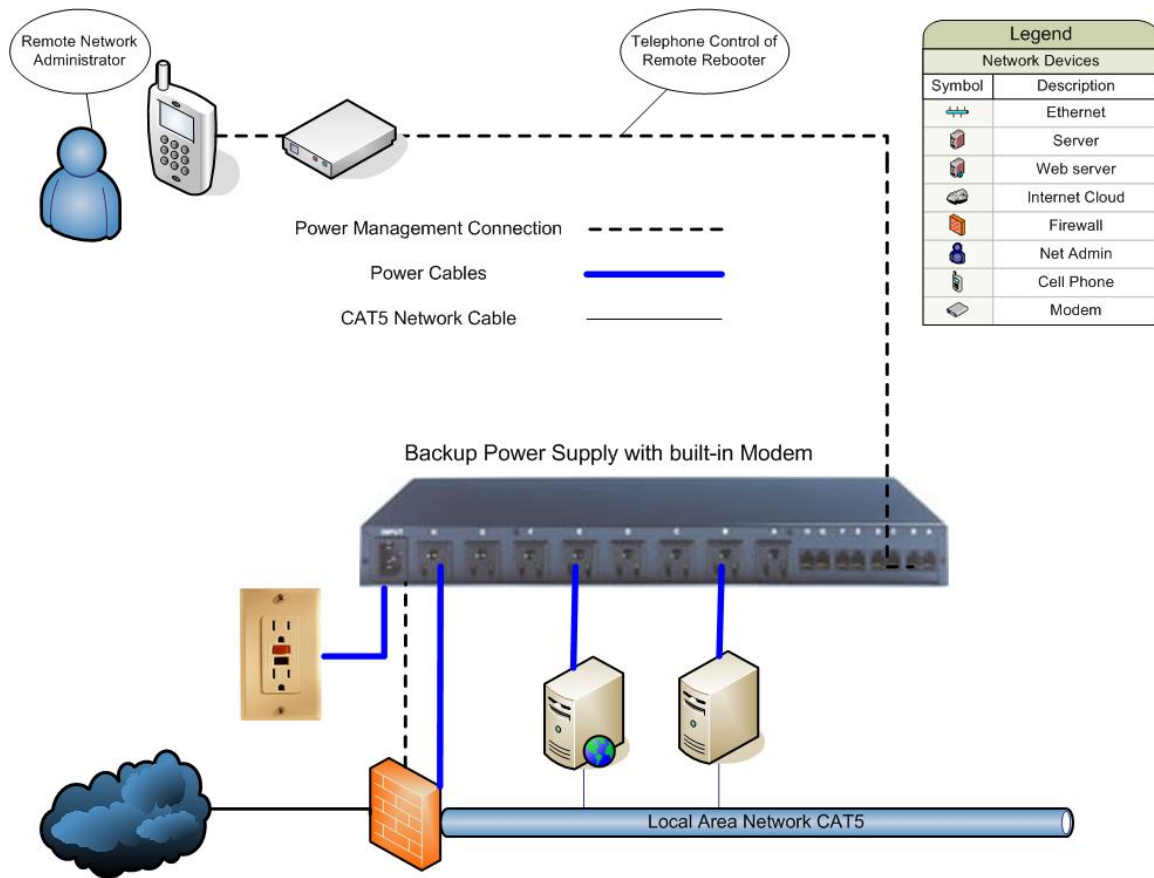


Figure 5.4. UPS with Built-In Modem for Remote Management

The second method for performing the power reset is using a touch-tone controller. The remote location houses a touch-tone controller either built into the UPS or connected in series with the UPS and a normal telephone device (see Figure 5.5). It is possible to configure the touch-tone controller to listen for a password, in the form of touch-tones, followed by a series of touch-tones, which would initiate a hard power-reset of the locked-up device. This method eliminates the need for modems, or in the event of a locked-up modem, it is possible to bypass it. The touch-tone controller is not an automatic management function and does require the remote administrator to call in to perform the reboot function. In addition to remote administrator assistance, phone lines at both the local and remote locations are required, but the touchtone controller allows other devices to share the Telco line, eliminating the cost of additional phone lines.

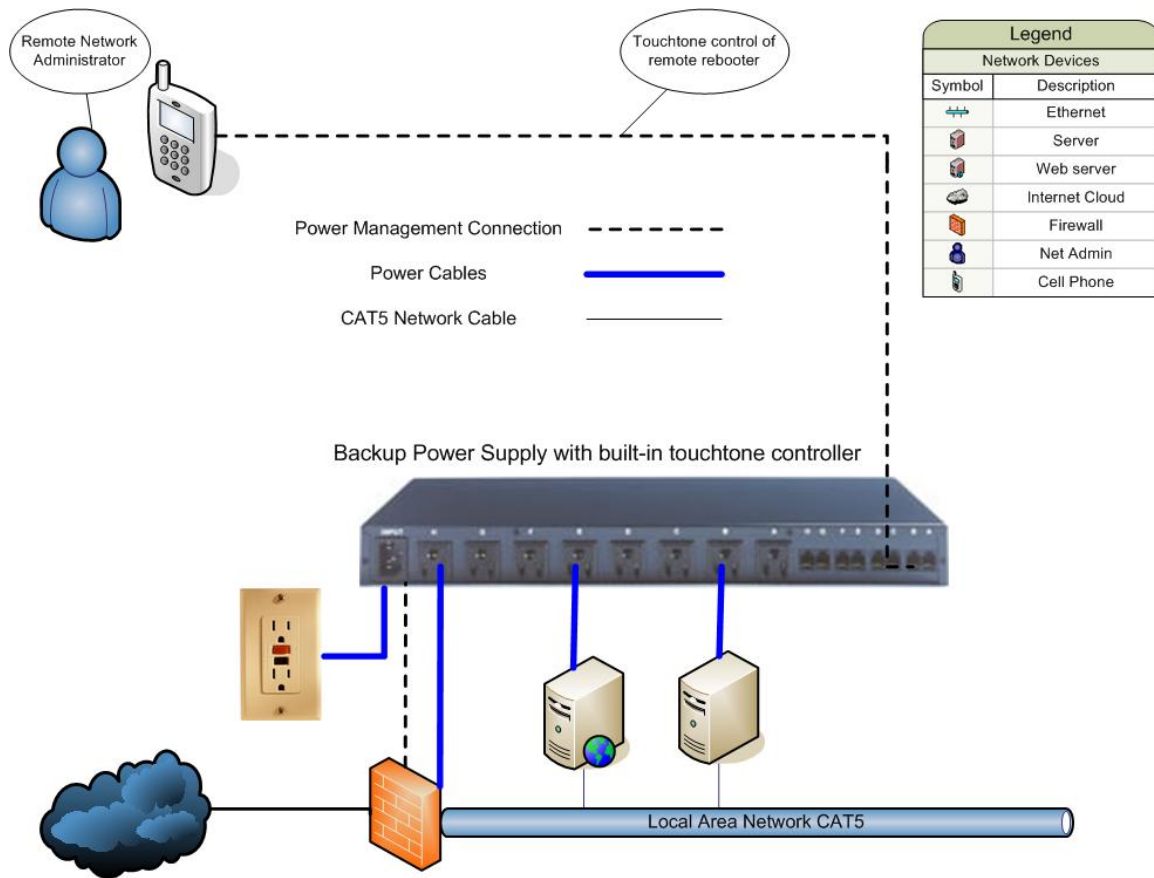


Figure 5.5. UPS with Remote Management via Built-in Touchtone Controller

A third method for remote power management is an automatic watchdog capability. By connecting a network device loaded with heartbeat software directly to the UPS with power management, the UPS can listen for the heartbeat of the server, and if not present, automatically perform a hard power reset of the associated device (see Figure 5.6). Therefore, the device loaded with heartbeat software will take care of its own rebooting, should it stop sending the heartbeat. The heartbeat software can also poll other network devices and initiate an automatic reboot command to the associated rebooter should any other network device become unresponsive. This minimizes downtime and eliminates the need for remote network administrator assistance.

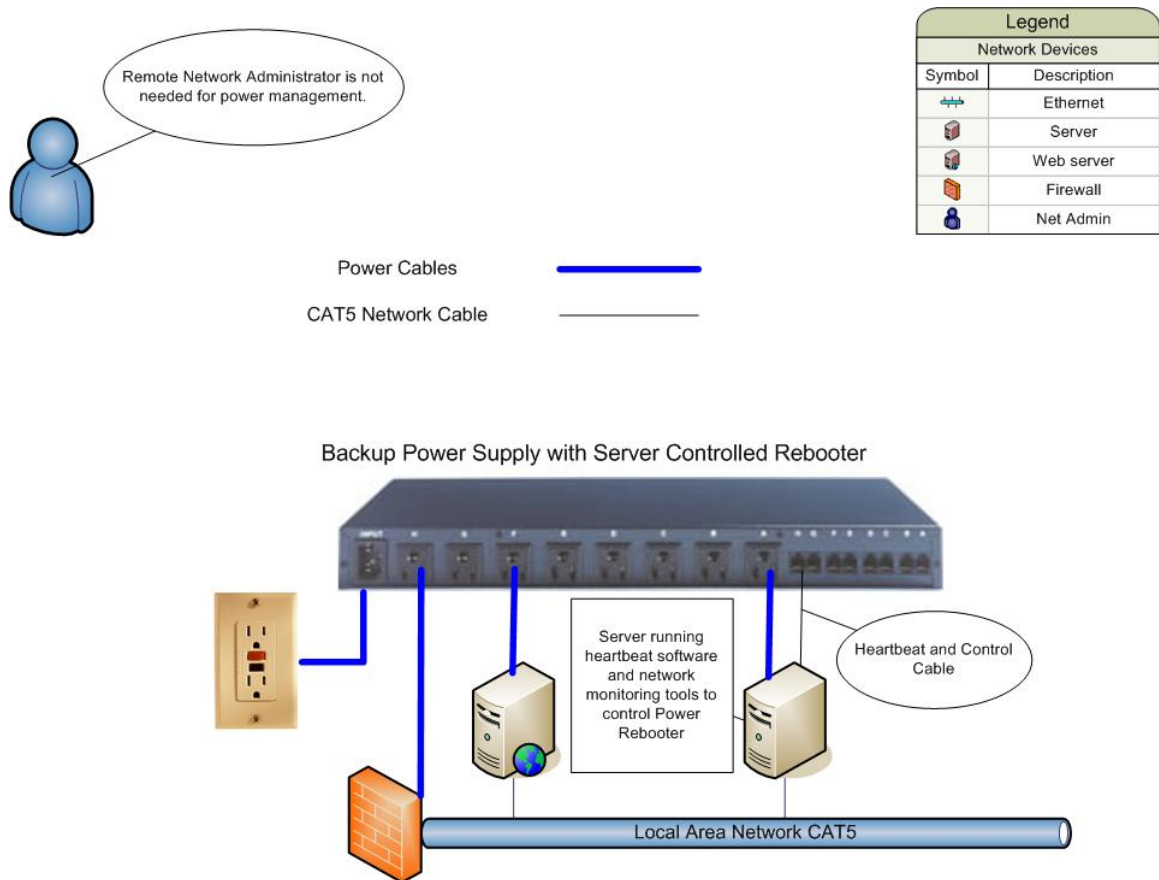


Figure 5.6. Backup Power Supply Controlled by Server Loaded with Heartbeat Software

A fourth method, nonexistent at this time, would be to incorporate network management utilities into the UPS (see Figure 5.7). A network administrator can then pre-configure the UPS such that each power outlet has an associated network device. Many different methods poll the network device for response, such as ping, DNS request, webpage request, POP3 request, and so forth. When a network device does not respond, the associated power outlet is automatically reset, restoring the locked up network device. This method minimizes downtime and eliminates remote administrator assistance.

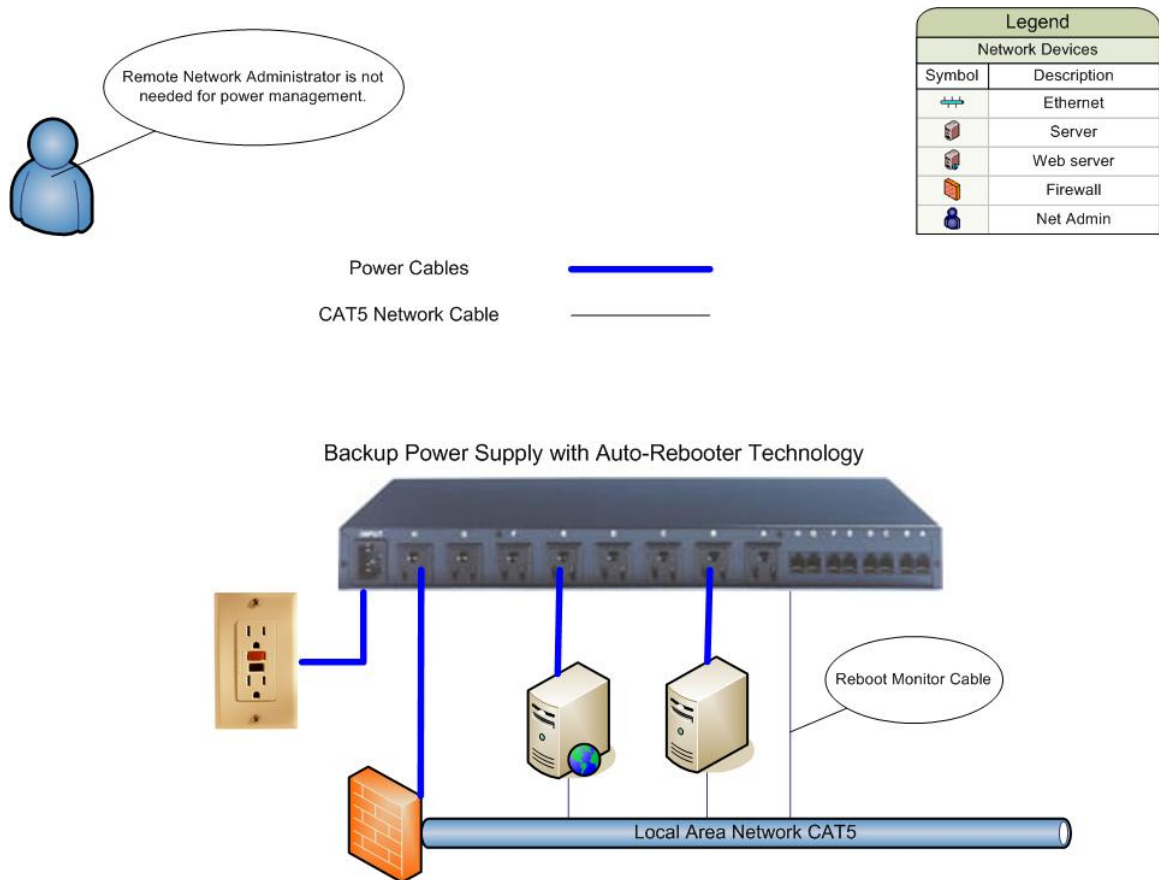


Figure 5.7. Backup Power Supply with Built-in Auto-Rebooter

It is always a good idea to have backup methods for remote power management due to the high-cost associated with downtime and technician on-site responses (see Figure 5.8). A mixture of in-band management (Internet) and out-of-band management (telephone) is also an excellent idea. The Internet interface is the least expensive to implement since the Internet connection already exists. The touch-tone controller is also very cost effective because it can share preexisting phone lines.



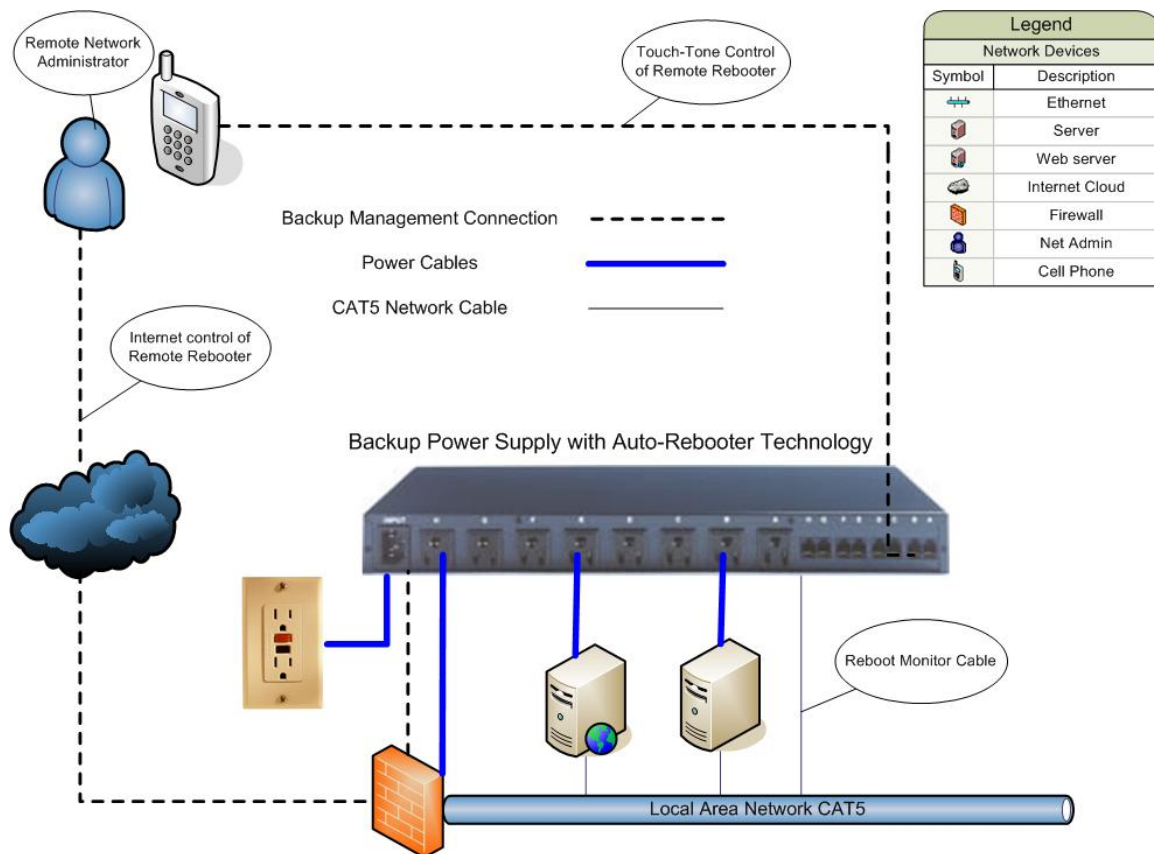


Figure 5.8. Backup Power Supply with Built-In Auto-Rebooter and Backup Management

#### D. CONCLUSION

Due to limited resources, the author was unable to build the auto-rebooter depicted in Figure 5.8. However, the author built a comparable unit by utilizing a known-good server loaded with heartbeat software and polling software, as depicted in Figure 5.6., also incorporating an external touch-tone controller, as depicted in Figure 5.5, as a backup method for management.

This known good server polls all associated network devices. If any should become unresponsive, the polling software sends the author a text message and waits for a response for troubleshooting. If the author chooses to not respond, or is unable to respond, within five minutes, the polling software will send a reboot command to the associated UPS outlet. Once the device is back online and responding, the software will

again send a text message stating total downtime. If the author does not want the software to wait for the full five minutes, it is possible to utilize the touch-tone controller and perform an immediate reboot.

This system has been online and functioning for four months now. Using the touch-tone controller, it was possible to share a pre-existing phone line eliminating the need for a second phone line. Prior to the design and installation of these devices, there would be approximately four lockups per week that needed a response. Use of this device has eliminated response to locked up network equipment, such as the wireless access points.

As the U.S. military continues to downsize, the need to do more with less is even more apparent. Unmanned networks continue to expand, and therefore, the demand for remote network management will become more critical to the success of those organizations. By using remotely manageable back-up power supplies, downtime is greatly reduced and the associated man-hours can be eliminated.

## **VI. CONCLUSION**

### **A. RESEARCH CONCLUSION**

This thesis investigates the many methods of remote network administration for both wired and wireless networks. It discusses the basic elements of wireless and wired networks, surveys the current wireless and wired management tools, and outlines methods for secure remote network management. Finally, this thesis introduces new methods for managing power control devices at remote locations.

A consideration from the very beginning of network design is the need for remote network administration. Designing a remote network administration solution for a pre-existing network is not as easy as designing a network with remote administration in mind. A star topology is a logical choice when designing a network in which remote administration is necessary.

The deployment of wired and wireless networks within the Department of Defense requires that security be the number one concern when designing the remote management platform. Many methods exist to manage both wired and wireless networks. However, it is imperative that some methods are not used, such as Telnet and SNMP v1, unless necessary. Transmitting passwords in the clear is never a good idea, especially when managing a mission-essential piece of network equipment over an untrusted network such as the Internet.

With the right utilities, managing network devices over an untrusted network can be just as secure as managing network devices on a trusted LAN. SSH tunneling is a reasonable starting point for remote network administration. By utilizing the port forwarding features of SSH client/server software, we can tunnel sensitive communications, ensuring that eavesdroppers cannot listen in. When economically viable, VPN technology is the best remote administration utility based on its functionality and security. Wireless networks can be operated and managed securely with the use of EAP-TLS. EAP-TLS enabled wireless devices are costly, but well worth the added cost.

Finally, during the research phase of this thesis a mock network was constructed and remotely administered to assist in identifying any potential weak points with remote administration. It was determined that the ability to manage power remotely for critical infrastructure was very limited. The design and implementation of remote power management hardware and software has greatly improved the overall uptime rates of all associated equipment, thereby greatly reducing the overall losses with downtime and eliminating the need for technician onsite assistance.

The Department of Defense networks span the globe. The cost to maintain and administer those networks is greatly reduced with secure remote network management. Having complete control of our unmanned network locations and all equipment within is crucial. This includes computers, servers, network infrastructure, and power control devices.

Complete remote network management allows for greatly reduced manning while increasing network uptime rates. Having secure remote network connectivity allows for centralized monitoring and administration. Centralized monitoring and administration, greatly reduces the associated costs of network management throughout the entire Department of Defense.

## **B. RECOMMENDATIONS FOR FURTHER RESEARCH**

The power control device depicted in Figures 5.7 and 5.8 requires further studies. Having an all-encompassing uninterruptible power supply capable of secure remote management and auto-rebooter technology is key to reduced downtime and associated man-hours.

## LIST OF REFERENCES

- Barnes, Bautts, Lloyd, Ouellet, Posluns, and Zendzian. *Hack Proofing your Wireless Network*. Syngress, 2002.
- Chlamtac and Lin. *Wireless and Mobile Network Architectures*. Wiley, 2001.
- Feibel, *Encyclopedia of Networking* (Network Press), Sybex, 2000.
- Forouzan, *Data Communications and Networking*, 2<sup>nd</sup> Edition, McGraw Hill, 2001.
- Gast. *802.11 Wireless Networks – The Definitive Guide*. O'Reilly, 2002.
- <http://www.citrix.com>, May 2004.
- <http://www.informit.com/articles/article.asp?p=101591>, May 2004.
- <http://www.microsoft.com/windowsxp/remotedesktop>, March 2003.
- <http://www.realvnc.com>, May 2004.
- <http://www.webopedia.com>, (March 2004.
- Kaufman, Perlman, and Speciner. *Network Security*. Prentice Hall, 2002.
- Northcutt, Zeltser, Winters, Frederick, and Ritchey. *Inside Network Perimeter Security*. New Riders, 2003.
- Osbourne. *CWNA, Certified Wireless Network Administrator*. McGraw Hill, 2003.
- Relevant security RFCs
- RFC 2716.
- RMON
- SNMPv1-3
- Tamar Dean, *Enhanced Network+ Guide to Networks*. Enhanced Edition, (Course Technology, 2003), 178.
- Tanenbaum. *Computer Networks*. Prentice Hall, 2003.
- [www.ethereal.com](http://www.ethereal.com).
- [www.GoToMyPC.com](http://www.GoToMyPC.com). March 2004.

THIS PAGE INTENTIONALLY LEFT BLANK

## **INITIAL DISTRIBUTION LIST**

1. Defense Technical Information Center  
Ft. Belvoir, Virginia
2. Dudley Knox Library  
Naval Postgraduate School  
Monterey, California
3. Capt Mark P. Sullivan  
Plattsmouth, NE